DAC BEACHCROFT

LEGALIGN GLOBAL

INFORMED INSURANCE 2022/2023

Resilience: new emerging threats challenge insureds and insurers

Resilience: new emerging threats challenge insureds and insurers

Insurers are facing more threats to their ability to operate and remain aligned with their customers' values than ever before. ESG-washing, supply chain issues, cyberattacks and ransomware are all part of this potent mix.

Many emerging threats are critical operational issues but they must also be nailed into the strategic planning by businesses. This means having the expertise to hand to identify the issues, analyse the threats they pose, create plans and put in place robust operational responses. For insurers, these present important challenges that they need to face up to in order to continue to deliver for their clients and for society.

ESG-WASHING

ESG-washing is a broad concept which refers to the risk that a company's Environmental, Social and Governance (ESG) credentials, strategic positioning and risk, or ESG related product attributes have been overstated and are misleading.

ESG related statements and disclosures come in a variety of forms, and can include product labelling and advertising, a company's prospectus or annual reports. Companies are also facing increasing levels of mandatory ESG disclosures, in particular climate related disclosures. Since the Task Force on Climate-related Financial Disclosures (TCFD) made its recommendations in 2017, the move towards mandatory climate reporting has gathered momentum. In the UK, mandatory TCFD-aligned requirements have been introduced across a large part of the economy. From January 2021 the FCA mandated TCFD disclosures for premium listed companies and extended this to standard listed companies in January 2022. New FCA rules came into effect in January 2022 compelling the largest asset managers and owners to make climate related disclosures. Since April 2022, large companies and LLPs are now also required to produce TCFD-aligned disclosures.

The list will grow longer and enforcement more rigorous, especially as national governments become more aligned in their approaches.

France has already gone further than most, passing a Decree that provides for a ban, from 1 January 2023, on promotional statements concerning carbon offsetting in all forms of advertising, unless "a greenhouse gas emissions report is produced for the product or service concerned, covering its entire life cycle."

This report must be accompanied by "the process by which these greenhouse gas emissions are first avoided, then reduced and finally offset." It is published on the advertiser's website, to which a link or QR code must be present on the advertising or packaging bearing the carbon neutrality statement.

When it put the Decree out to public consultation, the government explained that the Decree should ensure transparency and prevent any risk of greenwashing.

> *"There is a danger that when reporting does not have to be done in a prescribed manner, people can be tempted to be more cavalier."*
>
> Sarah Crowther
> DAC Beachcroft, London

BOLD ESG CLAIMS INVITE SCRUTINY

Claims of strong ESG credentials serve to attract investments and, potentially, increase share value. ESG statements and disclosures are increasingly being scrutinised by regulators, consumers, investors and activists in order to satisfy their own ESG objectives. Where these representations are found to be inaccurate, claims may follow.

The claims that could arise from ESG-washing are diverse. ESG-washing could result in a drop in a company's share price, triggering directors and officers (D&O) claims from investors who had relied on false representations. There is a daunting list of large derivative class actions brought by shareholders in the US on the basis of misleading ESG statements. ClientEarth's greenwashing claim in July 2022 against the Dutch airline KLM is a reminder that activists see tackling greenwashing as a key part of their strategy.

Regulators too have taken significant steps this year to crack down on greenwashing – the US Securities & Exchange Commission has targeted major banks with respect to misleading claims by managers of ESG funds, and German police raided the offices of DWS in May 2022 following allegations of greenwashing by the asset manager. The FCA has warned that financial products with ESG or financially sustainable characteristics should be accurately disclosed and marketed. With this increasing awareness of ESG-washing as a concept, insurers could find themselves looking at an increased frequency of losses.

"Perhaps the biggest risk is when ESG disclosures are made on a voluntary basis as a means to encourage investment," says Sarah Crowther, Partner and ESG claims lead at DAC Beachcroft. "There is a danger that when reporting does not have to be done in a prescribed manner, people can be tempted to be more cavalier."

Crowther says that, at present, the biggest concern in terms of ESG-washing lies in the "environmental" part of ESG.

However, there is also increasing focus on the "social" part. The Black Lives Matter movement in the US put a spotlight on diversity in societies around the world, including the UK.

In April 2022, the FCA finalised rules requiring listing companies to report information and disclosures against targets on representation of women and ethnic minorities on their boards and executive management. This followed a consultation on proposals to improve transparency around the diversity of company boards and their executive management teams.

The final element of ESG - governance – has always been what the boardroom is about. Poor governance lies behind the majority of claims against directors, explains Graham Ludlam, Partner in the Global Insurance Group at DAC Beachcroft: "It is however behind the E and S in terms of the new wave of social and investor attention".

He points to examples which he says show it is gathering pace. "The issue is being addressed in Germany, with a Supply Chain Due Diligence Act entering into force in January 2023. In February this year, the EU Commission also published a proposal for a directive on corporate sustainability due diligence which will introduce a duty on companies (and a related duty on directors) to identify, bring to an end, prevent, mitigate and account for negative human rights and environmental impacts in their own operations, and those of their subsidiaries and value chains, imposing a civil liability where there are failures to comply. These developments reflect a trend of formal legal obligations beginning to align with voluntary business human rights standards, such as the UN Guiding Principles on Business and Human Rights, placing a greater responsibility on parent companies for the activities of their group and supply chains."

D&O IN SPAIN

D&O insurers have been warned they should also look carefully at their Spanish books, as it is likely they will soon face a surge of claims. This is because a moratorium on insolvency declarations launched in March 2020, designed to deal with the COVID-19 pandemic, ended on 30 June this year.

Pablo Guillen, Partner at DAC Beachcroft in Madrid, says the firm expects significant insolvency-related claims over the next few months.

There is potentially a "huge amount" of claims, Guillen says, describing the current situation as a "perfect storm".

All the above coincides with the imminent approval of the draft bill amending the Insolvency Act, which aims to review the Spanish insolvency system that will affect debtors, creditors and potential investors.

Insolvency proceedings are expected to be filed from Q3 2022 and classification proceedings within insolvency proceedings (ie. where the liability of directors and officers will be examined) are likely to start in 2023.

FRANCE FEELS THE PRESSURE

Insolvency proceedings in France jumped by 34.6% in Q1 2022.

"After having reached extremely low levels thanks to the government's pandemic interventions, the number of bankruptcies in France is now close to its pre-crisis levels, without however exceeding them," says Christophe Wucher-North, Partner in DAC Beachcroft's Paris office.

"Although insolvency procedures could rise in France in the coming months, this would mainly be caused by the current supply chain and energy crisis and subsequent inflation. This should not have a significant impact on D&O claims, as to establish D&O liability requires demonstration of a management fault. The insolvency itself is insufficient for someone to be found liable on D&O grounds."

SUPPLY CHAIN ATTACKS, CRITICAL NATIONAL INFRASTRUCTURE AND OTHER KEY CYBER RISKS

Supply chain attacks pose an ever increasing and costly risk to businesses, targeting suppliers as a means for gaining access to, or disrupting, often higher-value companies. Such suppliers will be offering services or software which, if disrupted, may cause significant problems in terms of the supply chains of the firms they deal with.

Perhaps the greatest concern currently is a software supply chain attack given the vast numbers of customers that may be using that software. Should that be compromised, the downstream impact on all users could be very significant. Typically, with software supply chain attacks, threat actors look for unsecure network protocols, unprotected server infrastructures and unsafe coding practices.

A good example of the potential impact of supply chain attacks was the 2019 global NotPetya cyberattack which was spread by a centralised update to tax accounting software. It affected organisations around the world, with reports of over US$10bn of associated costs and damage.

The risks have never been higher due to new types of attacks, growing public awareness of the threats and increased oversight from regulators. In late 2020, for example, the SolarWinds attack, in which a malicious code was inserted into the software, infected around 18,000 customers downstream, including various US agencies such as the FBI, the Pentagon and the military. The estimated insured losses totalled around US$90m (according to BitSight) which is relatively modest because not all impacted entities held cyber cover.

For cyber insurers, the aggregate risk is significant, says Eleanor Ludlam, Partner in the Cyber & Data Risk team at DAC Beachcroft. For example, if a managed service provider (MSP)'s systems are compromised, and the threat actor is able to then move laterally into its clients' systems, there is a potential exposure for not only the first and third party cyber insurers of the MSP, but also the first party cyber insurers of all the MSP's customers.

"While there may be applicable exclusions in play, insurers could end up in a position where they are not only providing cover in respect of losses flowing from the originating breach at the MSP, but also for liability claims against the MSP which are brought by their customers that were breached as a consequence," Ludlam explains.

"Of course the additional attacks on the MSP's customers may also mean insurance claims for the customers' cyber insurers. This shows the potential aggregate risk to individual cyber insurers who insure MSPs and their customers, as well as the aggregate exposure across the cyber insurance market."

> *"The main targets today are now in the small and medium-size enterprise sectors, whereas two years ago the main targets were large corporates. Supply chain attacks are particularly problematic at the moment."*
>
> Kieran Doyle
> Wotton + Kearney, Sydney

When critical national infrastructure is targeted, the police and National Cyber Security Centre will take a particularly keen interest. The Colonial Pipeline ransomware attack of 2021 was a clear example of a risk to critical national infrastructure. The attack shut key conduits delivering fuel from Gulf Coast refineries to major East Coast markets. The US senate took a keen interest in the attack and said that the government and companies must work harder to prevent future hacks. These types of attack highlight how cyber can create systemic exposures to cyber and non-cyber insurers alike.

The boom in cyberattacks over recent years has resulted in many insurers significantly increasing pricing and demanding more stringent terms and conditions to underwrite a cyber policy. According to Marsh, the price of cover in the US spiralled by 130% in the fourth quarter of 2021 alone, while in the UK it jumped by 92%. It has also brought into focus the need for appropriate terms to deal with aggregate or systemic exposures, or exclude them entirely. The recent LMA Cyber War Exclusions are a good example of this.

"The impact is going to be significant for corporations, who will have to jump through more hoops to get cover," Ludlam says. "We are already seeing a greater number of organisations that have been unable to obtain cover given the hard cyber market at the moment. We have also seen insurers moving to co-insure risks and to exclude cover for ransom payments, for example."

Although France is highly exposed to cyberattacks, due to increasing premiums, the cyber insurance coverage rate among large companies decreased by 4.4% in 2021. In 2020, 251 large companies or 84% of organisations classified as such according to the INSEE typology - had taken out a cyber policy. In 2021, there were only 240.

In May, the UK government unveiled plans to improve the UK's cybersecurity protections through new legislation. The Product Security and Telecommunications Infrastructure Bill aims to ensure that "smart consumer" products – smartphones, televisions, Internet of Things devices (IoT) etc – are designed more securely at the manufacturing stage against cyberattacks.

The threat is significant. According to Ludlam, if the Internet of Things and smart devices continue to be developed with poor security standards, cyberattacks are likely to continue to increase.

Kieran Doyle, Partner at Legalign Global alliance firm Wotton + Kearney in Australia, says that the main targets today are now in the small and medium-size enterprise sectors, whereas two years ago the main targets were large corporates. Supply chain attacks are particularly problematic at the moment.

"This is having a huge impact for insurers as it comes with increased cost in terms of dealing with not just the attack but also third-party business interruption claims from clients," Doyle explains. "Those clients are also potentially triggering their own insurance policies, creating aggregation issues for insurers."

Cyber insurance prices in Australia have risen between 80% and 100% - in line with other geographies.

OPPORTUNITIES FOR INSURERS

All of these emerging threats represent huge opportunities for insurers who can get a handle on them. This is particularly so in the case of cyber insurance, which some believe could one day become the biggest line of business worldwide.

But the road ahead is tough. The risk is ever-changing, making it difficult to predict. And the problem of aggregation has yet to be solved.

It is often said by cyber brokers and insurers that we have not yet seen a "cyber-Katrina" - a massive loss event caused perhaps by the failure of a key piece of internet infrastructure. Until that happens, it will be difficult to judge how serious the problem really is - for insurers and insureds alike.

Facial recognition technology and scraping practices

Law enforcement has been increasingly reliant on new technologies to catch criminals, but these attempts sometimes fall foul of new regulations governing the use of data.

This issue came to the fore earlier this year, when the UK's Information Commissioner's Office levied its third largest fine ever, against facial recognition provider Clearview AI.

Clearview AI was fined £7.5m for scraping images of people from social media platforms and the web to add to a global database.

The company sells its services to law enforcement, which can send Clearview a picture of a suspect and be given a solid guess as to their identity. But John Edwards, the UK Information Commissioner, said Clearview's business model was unacceptable:

"Clearview AI Inc has collected multiple images of people all over the world, including in the UK, from a variety of websites and social media platforms, creating a database with more than 20bn images," he said.

"The company not only enables identification of those people, but effectively monitors their behaviour and offers it as a commercial service. That is unacceptable. That is why we have acted to protect people in the UK by both fining the company and issuing an enforcement notice."

Interestingly, this was a joint investigation with the Australian privacy commissioner, the OAIC, who made similar findings (i.e. that Clearview had breached similar provisions of the Australian Privacy Act) but the difference in enforcement and penalties between the two jurisdictions is stark.

According to Doyle, "the joint investigation highlights a clear difference between the two privacy regimes where, while the ICO has more power to consider financial penalties, the OAIC would be required to commence proceedings against Clearview to seek a penalty. Accordingly, the OAIC in this instance was limited to making declarations only of breach and, in effect, seeking undertakings not to repeat the breaches."

Doyle says further investigations are underway by the OAIC into retailers using facial recognition technology.

UK law enforcement had at least toyed with the idea of using the technology, which had been offered on a free trial basis to customers including the Metropolitan Police and the National Crime Agency. Those trials have been discontinued.

Contributors:

Sarah Crowther
scrowther@dacbeachcroft.com
DAC Beachcroft, London

Kieran Doyle
Kieran.Doyle@wottonkearney.com.au
Wotton + Kearney, Sydney

Pablo Guillen
pguillen@dacbeachcroft.com
DAC Beachcroft, Madrid

Eleanor Ludlam
eludlam@dacbeachcroft.com
DAC Beachcroft, London

Graham Ludlam
gludlam@dacbeachcroft.com
DAC Beachcroft, London

Christophe Wucher-North
cwuchernorth@dacbeachcroft.com
DAC Beachcroft, Paris

Click below to read our whole suite of new thought leadership:

- **Unlocking the potential of ESG: resilience, sustainability and collaboration**
- **Resilience #ESGwashing #cyberattacks**
- **Sustainability through technology: managing the transition #dataprotection #electricvehicles #telemedicine**
- **Collaboration #climateactivistlitigation #protectduty**

KEY CONTACTS

David Pollitt
Managing Partner
DAC Beachcroft
T: +44 (0) 117 918 2226
M: +44 (0) 7909 928 330
dpollitt@dacbeachcroft.com

Todd R Davies
Lead Partner
Alexander Holburn
T: +1 604 484 1799
M: +1 604 506 8294
tdavies@ahbl.ca

Helen Faulkner
Head of Insurance
DAC Beachcroft
T: +44 (0) 117 918 2225
M: +44 (0) 7841 322 480
hfaulkner@dacbeachcroft.com

Bastian Finkel
Partner
BLD Bach Langheid Dallmayr
T: +49 221 944027 893
M: +49 163 2829 330
bastian.finkel@bld.de

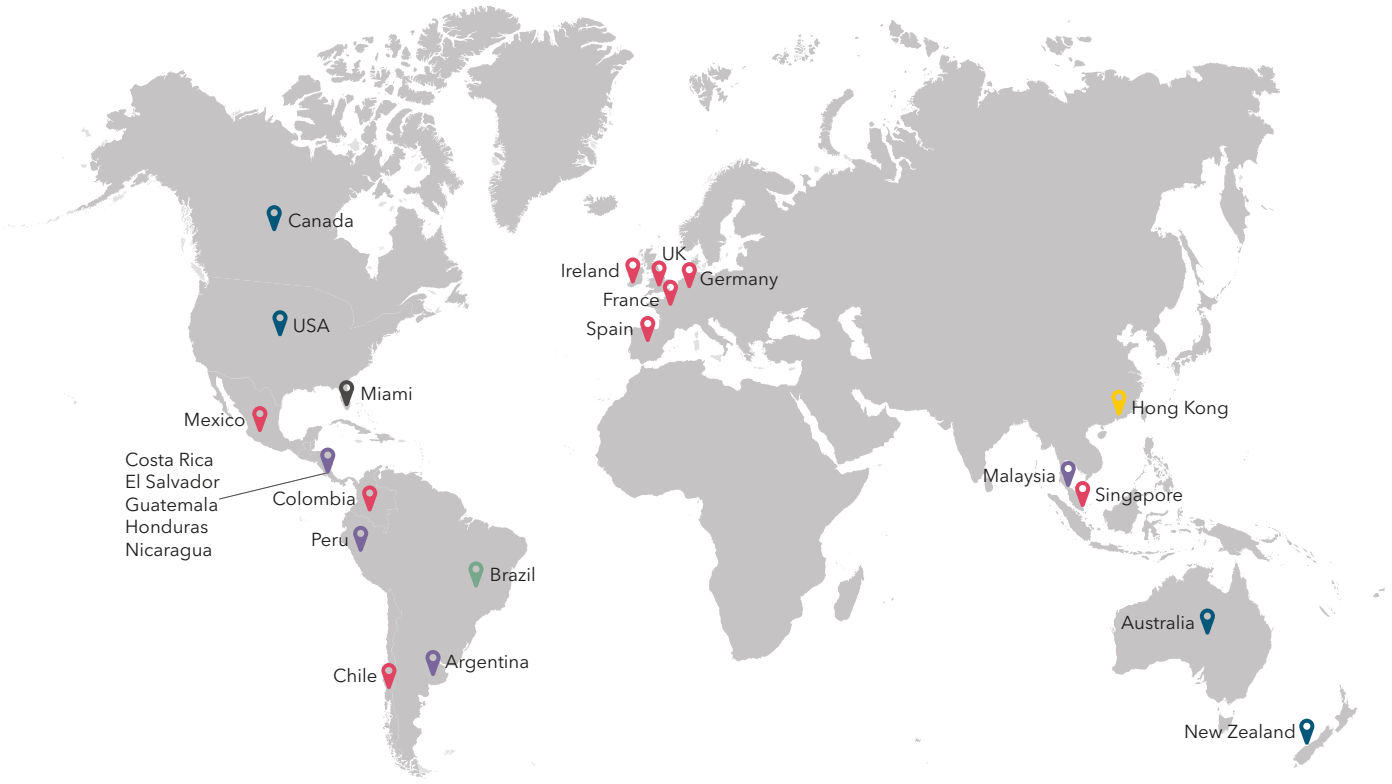
Craig Dickson
CEO
Claims Solutions Group
T: +44 (0) 121 698 5270
M: +44 (0) 7834 308 472
cdickson@dacbeachcroft.com

Daniel J McMahon
Chairman
Wilson Elser
T: +1 312.821.6147
M: +1 312.339.3895
daniel.mcmahon@wilsonelser.com

Charlotte Shakespeare
Senior PSL/ Editor
DAC Beachcroft
T: +44 (0) 207 894 6816
M: +44 (0) 7921 890842
cshakespeare@dacbeachcroft.com

David Kearney
Chief Executive Partner
Wotton+Kearney
T: +61 2 8273 9916
M: +61 4 1873 6196
david.kearney@wottonkearney.com.au

OUR GLOBAL REACH



DAC Beachcroft office
Representative office
Legalign Global
Associations
Best friends
Collaboration

insurance.dacbeachcroft.com

dacbeachcroft.com

Follow us: @DACBeachcroft

Connect with us: DAC Beachcroft LLP