Allianz

A BIBA BROKERS' GUIDE TO

Modern Risks

In association with

British Insurance Brokers' Association

DAC BEACHCROFT

We consider some key factors shaping the future of cyber insurance; the most prevalent types of attack being deployed by criminals; and guidance for businesses in combatting cyber threats.

Modern Risks

The digital revolution, coupled with unprecedented events in the socio-economic environment over the last two years, has resulted in a significant shift towards the insurance of intangibles.

Evolution is inevitable so we are pleased to provide insight on some of the more modern risks that business need to consider protecting against.

Cyber insurance offerings have become quite sophisticated with threat warning intelligence, forensics and communications often included, alas the risks have developed too so we look at what to be wary of.

Is brand and research more valuable than machinery and plant? For some it may be, as we consider insuring intangible assets.

We round off examining sustainable energy applications and their impact on claims.

A real forward-looking read!

Mike Hallam
ACII, Chartered Insurance Practitioner,
Head of Technical Services, BIBA

Contents

Insurance and the evolving cyber landscape

Christian Simpson

Lead Cyber Underwriter,
Allianz

Cyber insurance is still very much an emerging area for the industry since its first appearance in the 1990s but recent socio-political events are shaping the types of attack being perpetrated and, as a result, companies' cybersecurity requirements.

Overleaf, we consider some key factors shaping the future of cyber insurance; the most prevalent types of attack being deployed by criminals; and guidance for businesses in combatting cyber threats.

External influences

COVID

The COVID lockdown in March 2020 forced the large-scale move towards working from home, presenting new opportunities for cyber criminals. The rapid geographical spread of employees resulted in the wide distribution of office IT equipment, thereby introducing thousands of new routers, networks and personal WiFi connections. This, coupled with remote workers using their own (non-corporate) devices, led to increased exposure across companies' IT ecosystems. According to government data, 2020 saw a peak in cyber incidents, with 46% of businesses identifying an attack.[1]

Incidence of ransomware also accelerated during the pandemic, with criminals operating phishing scams involving information about vaccines or government financial assistance.[2] Perhaps unsurprisingly, ransomware ranked as the top cyber exposure of concern in the 2022 Allianz Risk Barometer.

Additionally, the various lockdowns prompted an increased reliance on video conferencing apps both for individuals and businesses. One which gained major prominence was Zoom – at the time a relatively underdeveloped and cost-free application. Companies started using the app en masse for business purposes and Zoom became a household name almost overnight, increasing from 10 million daily participants in 2019 to 300 million by October 2020.[3]

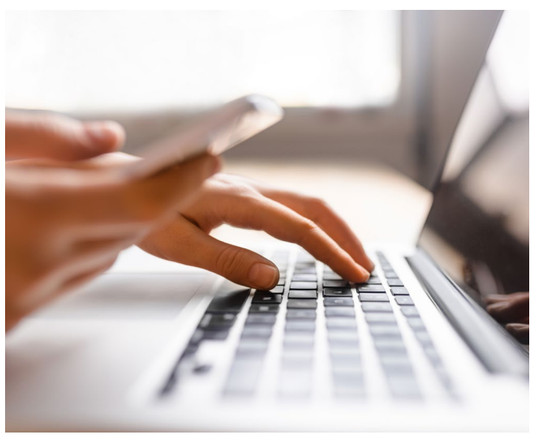
However, since Zoom was never designed specifically for corporate use, concerns soon surfaced around security vulnerabilities, such as the potential for any individual being able to gain access to meetings (known as 'Zoombombing'). Larger organisations with more mature security postures were less at risk, having processes in place for testing software or preventing the unauthorised installation of software.

46%

2020 saw a peak in cyber incidents, with 46% of businesses identifying an attack [1]

More than half of firms believe their exposure to attack has increased due to working from home arrangements

Ransomware ranked as the top cyber exposure of concern in the 2022 Allianz Risk Barometer



Cyber incidents can have huge repercussions for organisations, from financial loss to business disruption, reputational damage and fines. Given predictions that flexible working is set to continue, it's concerning that more than half of firms believe their exposure to attack has increased due to working from home arrangements.[4]

With many households retaining their dual function as both home and office at least some of the time, businesses will need to consider ways to improve their cyber security posture and minimise the risk of attack.

[1] Cyber Security Breaches Survey 2022. Cyber Security Breaches Survey 2022 - GOV.UK (www.gov.uk). Published March 2022.
[2] KPMG. The rise of ransomware during Covid-19. 2022.
[3] Forbes. In the Post Covid-19 world, Zoom is here to stay. In The Post COVID-19 World, Zoom Is Here To Stay. (forbes.com). February 2021.
[4] Survey of 1,000 UK firms from British Chambers of Commerce and Cisco. BCC FINDS RISING CYBER-ATTACK FEARS IN HYBRID WORKING WORLD (britishchambers.org.uk) January 2022.

> It's estimated that by 2030, there may be as many as 50 billion IoT connected devices globally.

Artificial Intelligence (AI)

Cyber criminals are exploiting AI for cyber-attack purposes, leveraging its ability to identify patterns in behaviour. For example, hackers can use machine learning (ML) – a form of AI - to support password guessing. By using ML, including something known as generative adversarial networks (GANs), it's possible to analyse a vast dataset of passwords and generate likely password variations.

So-called 'bad actors' can use AI to create personalised 'spear phishing' messages which target C-suite executives (CEOs, CCOs, etc) and either seek to obtain confidential information, or install malware on a device.

But AI can actually be used positively to thwart cyber criminals. Whereas monitoring cyber threats used to be an involved and time-consuming manual task, sophisticated AI systems are able to expedite the process without experiencing human fatigue and susceptibility to error. They achieve this by processing huge amounts of data to detect malware, run pattern recognition and automate defence responses.

Internet of Things (IoT)

It's estimated that by 2030, there may be as many as 50 billion IoT connected devices globally.[5] As more smart devices become connected in the Internet of Things, it will heighten exposure to cyber risk, especially where connected devices might have lower levels of security.

For instance, criminals may be able to gain access to an organisation's IT systems through employees' mobile devices or the company's connected kettle. Computerised controls, including alarms, environmental controls and CCTV can provide a back door for cyber criminals because they often utilise cost-effective but non-supported operating systems. Unsupported systems can be open to security threats and provide easy access to computer systems, bypassing firewalls and enabling hackers to gain access to a business's private or confidential data.

Russia-Ukraine war

At time of writing, there have been no confirmed Ukraine-Russia related attacks on the UK. However, there are fears that any heightened cyberactivity against Ukraine could signal an elevated threat for allies.

Previously, in June 2017, the NotPetya attack on Ukraine spread beyond its borders and impacted upon some UK operations. It's thought to be the most costly cyber-attack in history. More recently, a series of distributed denial of service (DDoS) attacks in February, which attacked Ukrainian banking and defence websites, was attributed to the Russian military intelligence agency GRU.[6]

Such attacks have led the UK's National Cyber Security Centre (NCSC) to issue guidance for organisations on how to improve their cybersecurity resilience.

Outsourcing of IT/ security

Another worrying trend is the amount of attacks on managed service providers (MSPs). Many companies outsource their IT services to an MSP, not considering that even MSPs themselves are not immune to cyber threats. In fact, since MSPs may support hundreds of customers, criminals see this as a way of attacking multiple companies via a single vector. The SolarWinds attack in 2020 was one such example, when hackers broke into the company's systems and ended up impacting around 20,000 of its customers. The attack was described as 'the largest and most sophisticated attack the world has ever seen'.[7]

It's important for organisations to undertake due diligence when selecting an MSP, such as understanding what security mechanisms they deploy, how they back up customer data and whether they have ransomware insurance, to name just a few.

[5] Statista. https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/
[6] https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine. 18 February 2022
[7] Reuters. SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president. February 2021.

Implications for the insurance industry

The global cyber insurance market is forecast to grow to $20.6bn (£15bn) in GWP by 2025 [8] but the industry is very much still learning as the cyber landscape continually evolves. Cyber carriers are receiving more claims, due to both higher take-up of cyber insurance and the number of incidents.

Allianz Global Corporate & Specialty saw claims rise from almost 500 in 2018 to more than 1,100 in 2020.[9] The recent surge in ransomware claims has driven up cyber insurance pricing by 92%.[10]

Cyber threats, including ransomware, are becoming increasingly more complex. Therefore, insurers will want to be assured that policyholders are taking appropriate steps to equip themselves against cyber threats. These include use of multi-layered protections like Virtual Private Network (VPN) technologies in conjunction with multi-factor authentication (MFA). This helps to verify the identity of users with a second factor before granting access to corporate systems and applications. Without proper use of MFA, it can be fairly simple for even novice cyber criminals to gain unauthorised access.

How can businesses best mitigate against cyber security threats?

In addition to the measures mentioned above, organisations can strengthen their security posture in a number of ways, including:

- training employees on how to recognise and report a potential breach
- implementing robust password security and considering the use of password manager tools
- using data encryption methods and ensuring data is backed up
- use of network segmentation; ensuring users only have access to relevant systems. Also using methods such as firewalls or airwalls (which securely connect anything, everywhere) to prevent an attack from spreading
- having a documented process for patching, including factoring in how quickly these can be implemented following a critical update
- maintaining a list of trusted applications and software, ensuring that anything not on the list cannot be used or installed
- allocating budget for IT security and infrastructure spend; the cost of this would be dwarfed by the repercussions of any cyber security breach
- having a current, robust business continuity plan in place.

$20.6bn

The global cyber insurance market is forecast to grow to $20.6bn (£15bn) in GWP by 2025[8]

[8] GlobalData. Cyber insurance industry to exceed $20bn by 2025, says GlobalData - GlobalData. 6 July 2021.
[9] AGCS. Allianz Risk Barometer 2022 - Cyber incidents | AGCS
[10] Marsh. Global Insurance Market Index 2021.

Can't touch this – insuring intangible assets

Glen Clarke

Head of Strategy and Propositions, Allianz

Until fairly recently, the concept of insurance was primarily concerned with the risk transfer of physical assets. However, the digital revolution, coupled with unprecedented events in the socio-economic environment over the last two years, has resulted in a significant shift towards the insurance of intangibles.

Go back fifty years and companies measured their value in tangible assets, such as their premises, stock and equipment. But for today's businesses, the value of their intangible assets has soared and in many cases, overtaken the value of their physical resources; examples include brand, reputation, intellectual property and data. Predictions vary but certain reports state that intangible assets account for 90% of portfolios among Standard & Poor's 500 companies.[1] This compares to just 17% in 1975.

Why has this shift occurred?

One factor is the digital revolution. Businesses of all sizes are increasingly moving their operations online to match consumer needs and behaviour. Adopting an e-commerce model also has the benefit of expanding a business internationally and reaching new customers and markets.

The COVID pandemic has undoubtedly accelerated the move online, with a large-scale trend towards home - and flexible working. This has necessitated the widespread adoption of digital technologies, plus the proliferation of video conferencing apps. Moving employees and equipment out of offices has introduced new access points for vulnerability and brought risks such as cyber-attacks and data theft sharply into focus. In turn, these risks can threaten intangible assets such as reputation and brand value.

[1] The Visual Capitalist. The Soaring Value of Intangible Assets in the S&P 500.

How can businesses manage their intangible assets?

The first step for business leaders is to identify and understand the value of their intangible assets. Some reports[2] place human capital, reputation and brand and intellectual property as the most valuable type of intangibles. A good approach to gauging worth is to base the value on the cost of replacing or redeveloping the asset. Alternatively, it's sometimes possible to use current data regarding competitors' transactions, where this is available in the market. Patent and trademarks are one such example.

A challenge with accounting for intangible assets is that only acquired assets, or those with a stated value are recorded on company balance sheets. Another consideration is that the value of an intangible asset can vary over time. Brokers are best placed to advise on suitable insurance solutions available for intangible assets, from protection against associated legal costs, loss of brand equity and the theft of intellectual property. As with traditional insurance products, insurance consumers will need to be clear on what is and isn't covered under their policy.

Being prepared for a crisis

Another potentially useful exercise can be for companies to test their resilience, in order to prepare for a real event. This could take the form of a crisis communications exercise or a cyber-attack simulation. Such rehearsals can be constructive in understanding what actions would be needed in a real-life scenario, plus the extent and implications of the loss.

[2] KPMG. Protecting intangible assets: Preparing for a new reality. p.15

What role do insurers play?

Whilst intangible assets can represent high values, assigning an accurate financial value isn't straightforward. By comparison, tangible assets are relatively easy to insure.

Granted, the insurance industry has already evolved to create solutions for intangible risks, including cyber, intellectual property and employee negligence covers. However, with the current trend likely to continue, the industry will increasingly need to develop covers to protect the economic value derived from intangibles.

Clever use of data and analytics will be vital for developing such solutions, especially if the industry is to move away from generalised products towards those which can be tailored according to a customer's specific need. Such data could also support the development of security incentives along different product lines, in a similar way that telematics data is used in motor policies.

Summary

All evidence points to the growing need for more insurance solutions which cater for intangible assets. This relies on a number of factors, including collaboration between risk managers and insurers, plus the expertise of underwriters and brokers working closely with customers to truly understand and advise on best cover for the insurable risk.

Getting a grip of intangibles - changing law in a changing world

Campbell Dye

Partner, DACB

There was a time – not so long ago - when life seemed more certain and predictable. Before COVID-19 and the Ukrainian war were we too complacent? Of course, for those involved in the identification and management of risk, the world was never like that and has, by definition, always been uncertain. That is why insurers have spent decades developing ways of understanding, analysing and pricing risk to give their customers the best cover available for a decent price and an acceptable return.

Although historically risk has been uncertain, it has, to some extent, been knowable – if you sail a ship there's a chance it will sink in a storm. If you develop and market a pharmaceutical, there is a risk there could be serious unforeseen side effects. If you drive a car you might be in a crash.

As we race through the third decade of the third millennium, those known unknowns remain but, as commerce becomes more complex and technology becomes ever more integral to our daily lives, there's a new breed of risk – a category of intangible risk which lurks unforeseen and unknown within everyday business activity across multiple sectors, and which can come back to bite the unwary with rapier sharpness.

Take, for example, a fictitious start-up – "Sweetness and Lite" – an online shop selling bespoke confectionery which is low sugar, but delicious. Start-up sales have been strong and the reviews on the website are great. What could possibly go wrong? Well, in a climate where the business and its owners and managers are clickably critiqued by the world in an instant, here are a few thoughts:

- What about the original DIY website, cobbled together one night by the founder in her spare bedroom? It turns out those great pictures she found on Google images have metadata embedded in them and are subject to copyright. The rights holder makes a claim.
- The web advertisement they produced for the UK and Europe has been picked up by social media in the Middle East and is getting millions of views. The contract with the "talent" in the advertisement had geographical restrictions on use. A claim for damages is threatened.
- A junior social media executive with the business attempts a humorous comparison with the products of a multinational competitor. She tries to laugh off their allegation of a breach of the Comparative Advertising Regulations but they are not smiling.
- Finally, our hapless founder, fuming at the disproportionate threats of litigation by her competitor, sends a late-night tweet, making all kinds of lurid allegations about the competitor and its CEO. Claims for defamation and invasion of privacy soon make their way to her inbox.
- Consider the benefits of taking out insurance cover for construction, operational and/or business interruption risks.

One thing seems certain, we are not going to go into reverse any time soon.

The proliferation of media platforms; the exponential expansion of content and the ever-broadening scope of engagement have taken traditional and well-established legal concepts – defamation, intellectual property etc - and combined them with new and developing areas of law (such as cyber, privacy and harassment) to create a landscape where it can be difficult to get a real idea of what risks lie where.

Intellectual property for example, has always been a fairly specialist area for policy-makers, although many general liability policies do provide cover for copyright and trademark infringement. In fast-track culture where cut and paste images are immediately available, the risk of inadvertent (or deliberate) use of someone else's copyright material should not be dismissed.

But what about technological sub-components? I have seen cases where a designer was threatened with legal action for his use of a particular font. I have also acted for the designers of the album cover for a major international rock band because their design was a little "too closely inspired" by a dead Belgian artist.

The digital planet is also seeing the conflation of a number of different causes of action or legal principles. While the Defamation Act 2013 has certainly seen a reduction in the number of libel and slander cases before the English Courts, the expansion of the tort of privacy has given claimants new and novel ways of complaining about things they don't want said about them.

So, for example, a claim in defamation might fail because the words were true, but there may still be a liability if those true words expose something of the claimant's private life. Keep an eye out too for changes in what may, or may not, constitute a defamatory meaning as society cartwheels through rapid and significant moral and social change around sexuality, race and gender identity.

Keeping a grip on these intangible risks can be tricky but talking about their potential and the impact upon the customer is necessary. One thing seems certain; we are not going to go into reverse any time soon.

Securing the future of renewable energy

Steve Kelly

Head of Engineering, Construction & Power

The use of renewable energy is accelerating, according to the International Energy Agency, with 2021 proving to be a another record year in new renewable energy generation capacity.[1] Renewables, such as solar, wind and hydro, are viewed as key contributors to the UK's progress towards its 2050 net zero ambition.

[1] International Energy Agency Renewables 2021 - Analysis and forecast to 2026. p.14

Insurers can act as key enablers in the advancement of renewable energy use, through offering a portfolio of relevant products and solutions, and through making responsible investments. However, insurers also need to be assured that basic good risk management is in place for renewable technologies, for the fair selection and pricing of risk. As the renewables energy market continues to grow, so does the requirement for robust risk management methods. This article examines some of the key areas for focus.

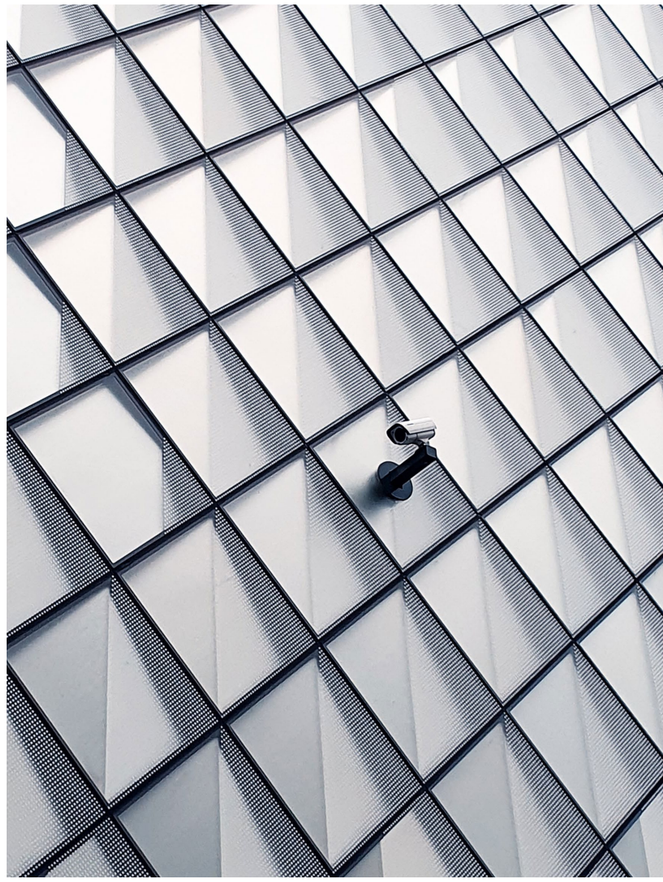
Site security

Physical security methods have not necessarily kept pace with emerging renewable and sustainable technologies. More conventional power installations, like coal and gas power stations, have historically had stringent perimeter security in place. This is less common with solar sites and so it can be easier for trespassers to breach perimeters and gain unauthorised access.

Criminals primarily target the cabling for the value of its metal; this can be costly to replace but also can have financial repercussions in terms of business interruption. Hence, site security is of the utmost importance for such installations.

By nature, commercial ground mounted solar panel systems are often installed in rural, isolated areas. This adds to the threat of criminal activity since any lawbreakers are less likely to be apprehended in the act. Furthermore, once access has been gained, thieves benefit from the solar equipment being located in one place, making it easier and quicker to steal and make an escape.

> Insurers need to be assured that good risk management is in place for renewable technologies, for the fair selection and pricing of risk.



Allianz became the first insurance partner of Solar Energy UK in March 2022, allowing the company to better support its solar power insurance customers and help educate members on the key risks the industry faces.

Site planning

Renewable energy installations, such as ground-mounted solar panels, generally require large physical areas, which can be a challenge given the UK's limited land mass. This, coupled with the appetite for Britain to achieve energy independence, has resulted in the relaxing of some planning laws.[2] Risks present themselves where installations are built in unsuitable areas, such as on flood plains. Flood risk assessments undertaken during the planning stage can help to identify such an issue, and furthermore are legally required for developments planned in flood zones 2 or 3. There have also been instances of solar farms being built on sites of special interest, where it was not possible to excavate sufficiently to secure the foundations. The resulting instability poses a real safety threat during periods of extreme weather.

Another potential pitfall is where planning has been agreed for solar sites, but not for associated security and weather protection. For example, erecting fencing and installing CCTV may be prohibited, leaving a site vulnerable to criminal activity. Plus, leaving a site without the requisite weather protection can result in a deficient and hazardous installation.

An opportunity for insurers?

It's in insurers' best interests to know the risks they underwrite are well managed; therefore it makes sense to become involved in the risk management process as early as possible. This could potentially see insurance companies shift into a more consultative role in the future, to provide guidance during the planning and construction stages, as well as during the operational lifecycle.

Similarly it may be beneficial for insurers to partner with renewable energy trade associations and professional bodies, in order to provide education and guidance to members on risk management practices.

Top tips for security

- Prior to construction, consult with the local planning authority so they can arrange an appropriate desk-based assessment and potential field evaluation.
- Once constructed, install high perimeter fencing and screening, with fully secured access points and alarms.
- Consider installing CCTV, plus remote/overnight CCTV monitoring off-site where possible, to act as both a deterrent and information gathering device.
- Incorporate flood mitigation methods into planning and ensure flood risk assessments are undertaken for high risk zones.
- Consider the benefits of taking out insurance cover for construction, operational and/or business interruption risks.

Summary

With the phasing out of fossil fuels, renewable energy has emerged as the global solution. This requires renewable energy technology to be safe, fully operational and fit for the future.

Operators of renewable energy sites have a responsibility in ensuring due diligence is undertaken when selecting prospective sites, plus guaranteeing that robust risk management practices are in place following construction. Through insurers and customers working together, risks can be planned for and managed, reducing the likelihood of a claim.

For more information visit allianz.co.uk/riskmanagement

[2] The Guardian. Tories plan big expansion of wind farms 'to protect national security' | Renewable energy | The Guardian 13 March 2022.

Shedding light on solar panel claims

Jennifer Pateman

Senior Associate, DACB

Toby Vallance

Partner, DACB

Aside from the omnipresent concerns around climate change, the recent huge increase in energy prices and the volatile gas market means the UK is inevitably focusing on a move towards more renewable sources of energy. Solar power has become a core part of the UK's renewable energy sector, and consequently insurance on commercial roof top and ground mounted solar projects is essential.

Solar panels comprise several individual solar cells which generate electricity from sunlight. Any electricity generated can then either be used onsite, stored or exported to the National Grid for distribution.

With the increase in the installation of solar panels comes an increase in first party property damage claims arising from theft of cablings, breakdown claims as a result of equipment age, weather events (including lightning) and fires.

Technological advancements raise issues around replacing damaged equipment and backward compatibility to replace parts of an original system cannot be assumed.

Damaged solar panels may require repair, substitution with an exact match or in some circumstances a full replacement of the system.

This may cause issues where panels which are several years old are damaged, and the policy provides cover for replacement on an 'as new' basis, with betterment excluded. There are also financial consequences of damage to solar panels. Commercial solar farms generate revenue by selling electricity to the National Grid, so it's easy to see how downtime can cause significant business interruption losses.

In addition, a solar farm may generate revenue by trading Renewable Obligation Certificates which are issued as part of an Ofgem scheme to incentivise the use of renewable energy. Alternatively, if solar panels are installed on a commercial building to generate power onsite, any interruption will result in the business having to buy power off the grid at great expense. Understanding how a business uses its solar power is key to accurately measuring any business interruption losses following physical damage to solar panels. Seasonality and location are also important considerations when projecting loss of revenue.

In order to assess the impact of these factors, the power generation history of solar panels can be analysed, along with any undamaged panels that are in close proximity. As is usual for business interruption claims, any savings made should also be taken into account.

The solar industry has seen rapid growth in recent years, and this will no doubt continue with technological advances and the ESG spotlight on renewable energy sources. Inevitably, this will result in an increase in claims, which will in turn require a deeper understanding of solar power and how solar businesses operate across the

BIBA Guides

British Insurance Brokers' Association

BIBA's supplements are brought to you through a partnership of BIBA, Allianz and DAC Beachcroft.

We hope that you find DAC Beachcroft's legal expertise, Allianz's industry knowledge and BIBA's desire to share these with you helpful.

We welcome ideas for future subjects.

BIBA cannot guarantee, and does not accept any responsibility or liability for the accuracy or completeness of the content by other authors.

Here are just some of BIBA's guides, provided in association with DAC Beachcroft LLP and Allianz: Click here to view all

- The Future of Mobility
- Key Brexit Business Considerations
- Risk Evolution
- Insurance Fraud Landscape
- Digital Technology
- Sustainability
- A Legal Round Up
- Claims Inflation Trends
- The Role of Engineering Inspection & Maintenance
- Employers' Liability Insurance

British Insurance Brokers' Association
8th Floor, John Stow House,
18 Bevis Marks, London EC3A 7JB

Member Helpline:
Tel: 0344 7700266
enquiries@biba.org.uk
biba.org.uk

Allianz Insurance plc
57 Ladymead, Guildford,
Surrey GU1 1DB
https://www.allianz.co.uk/

DAC Beachcroft LLP
25 Walbrook,
London EC4N 8AF
https://www.dacbeachcroft.com/

Produced by SandisonPay
01159 056364
www.sandisonpay.co.uk