A BIBA BROKERS' GUIDE TO

BUSINESS INTERRUPTION INSURANCE

2018 – Issue 4

BIBA
In association with

DAC beachcroft

Allianz

WELCOME

Inside this guide we take a broad look at business interruption and ways to help clients understand and mitigate their risks.

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.

Business interruption (BI) is one of the most complex insurances that a business will need to buy. For some time BIBA has been working to raise awareness about the consequences and causes of underinsurance and there are several issues in relation to BI. In fact the Chartered Institute of Loss Adjusters found in its 2017 survey of loss adjusters who had handled BI claims that there were a number of significant causes that resulted in underinsurance on BI covers. These included misunderstanding the insurance definition of Gross Profit, lack of explanation about how BI works, underestimating growth and not taking account of seasonality to name a few. This variation simply serves to highlight the complexity of this type of cover that can be represented by a single line in an insurance policy schedule.

Add to this the changing nature of risk and the rise of cyber and terrorist non-damage interruption to business and it is clear that there can never be too much information published about this class of insurance.

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

NON-DAMAGE BUSINESS INTERRUPTION - THINKING OF THE NEIGHBOURS

The 2017 surge in terrorist attacks on UK soil shone a spotlight on the absence of cover for terrorism-related non-damage business interruption (NDBI) losses in traditional policies - particularly for SMEs. The new Counter-Terrorism and Border Security Bill 2018, currently making its way through Parliament, is designed to close this gap so both businesses and insurers are following its progress with interest.

AUTHOR:
JAMES REDFORD
PROPERTY UNDERWRITING MANAGER, ALLIANZ

However it's not just terrorism-related events highlighting the topic of non-damage business interruption. Other recent incidents such as the tragic case of Grenfell and the chaos-inducing 'Beast from the East' have shown how contiguous businesses can be affected by business interruption (BI) events, often suffering revenue losses even when they themselves have not suffered physical loss.

This loss may occur through either denial of access, as in the case of Grenfell, or through loss of attraction – for example where a business experiences a decline in custom due to a nearby physical interruption event. A case in point is the recent Novichok poisoning in Wiltshire, which resulted in many shops unable to open or trade as usual during the investigation and clean-up.[1]

Whereas larger businesses often have the financial stability and requisite disaster recovery plans in place to restore normal operation quickly following such an event, this might not be the case for SMEs. Smaller businesses may simply not have adequate cash reserves to withstand a lengthy period where they are unable to trade as usual, and therefore are arguably more likely to be significantly impacted by a business interruption. With many enterprises of this type tending to be entrepreneurial, SMEs are also at greater risk of underinsuring, with around 44% inadequately insured for business interruption loss[2] and fewer than 3% of SMEs taking up terrorism cover.[3] It's important for businesses to ascertain the correct level of cover required and select an appropriate indemnity period. Not doing so could lead to business owners being out of pocket.

In 2018, BI topped the Allianz Risk Barometer[4] for the sixth consecutive year as the key concern for businesses globally, suggesting a need for greater support in this area. Whilst Pool Re's extension of terrorism cover to include NDBI will be welcomed by many, it remains crucial for businesses to consider any event which could slow or completely halt their ability to carry out business as usual.

1 BBC News, "Will Salisbury ever recover from the Skripal poisoning?" https://www.bbc.com/news/uk-england-43839176
2 Chartered Institute of Loss Adjusters 2016/17 survey
3 Insurance Business UK: https://www.insurancebusinessmag.com/uk/news/kidnap-ransom-terrorism/terrorism-insurance-gets-uk-breakthrough-95677.aspx
4 Allianz Risk Barometer 2018 [PDF], Allianz Global Corporate & Specialty (AGCS)

INSURANCE OF BUSINESS INTERRUPTION LOSSES CONSEQUENT ON TERRORISM ATTACKS

Five out of the ten most costly global terrorist attacks of recent times have occurred in the UK. Terrorist attacks can have far reaching effects, interfering with the businesses of a multitude of commercial organisations, many of which will not have been the primary target of the terrorist attack.

This can lead to gaps in business interruption cover, which Parliament is currently looking to address. Most commercial policyholders will have little interest in whether an event which impacts their business amounts to terrorism, or some other malicious or accidental act. All they want is to ensure they are covered for loss of profits which might flow from such events.

TERRORISM INSURANCE IS NOT A COMPULSORY FORM OF INSURANCE IN THE UK.

Across Great Britain, more than £2 trillion of exposure to terrorism risks is underwritten through the Pool Re[1] scheme which applies to eligible commercial property risks (including buildings, contents, construction projects, plant and machinery, amongst other things), located in Great Britain.

Commercial property insurers will generally exclude acts of terrorism from their material damage and business interruption policies, but then offer terrorism cover for an additional premium.

For those policyholders who elect to have terrorism cover, losses arising out of acts of terrorism will be met by the insurer up to a threshold agreed with Pool Re. Losses exceeding that threshold are reinsured back to Pool Re (and ultimately the Government, if Pool Re's reserves become exhausted).

1 Pool Reinsurance Company Limited

AUTHOR:
JAMES DEACON,
PARTNER AT
DAC BEACHCROFT LLP

The Pool Re Scheme extends to risks of:

- Loss of or damage to property in Great Britain resulting from or consequential upon acts of terrorism; and
- Any loss which is consequential upon such property damage.

It will be evident from this that for a policyholder to benefit from terrorism cover, they must suffer some physical damage to their commercial property, and can only claim for business interruption losses, where such losses are consequent upon that physical damage.

Before cover under the Pool Re scheme will respond to a loss, the Government (or, alternatively, a Pool Re tribunal) must certify that the event concerned was caused by an act of terrorism.

Terrorism is defined by the Reinsurance (Acts of Terrorism) Act 1993 as:

"Acts of persons acting on behalf of, or in connection with, any organisation which carries out activities directed towards the overthrowing or influencing, by force or violence, of Her Majesty's government in the United Kingdom or any other government de jure or de facto".

As terrorism risks have evolved, so too has the scheme. In July 2002, the biological, chemical, radiological and nuclear contamination exclusions were removed. Most significantly, from 1 April 2018, terrorism cover has started to be offered as standard for material damage and consequential business interruption losses, caused by cyber terrorism.

But, the cover provided for business interruption losses is still limited. The London Bridge terrorist attack in June 2017 highlighted a significant problem with terrorism cover.

Following the initial terrorist attack, a police cordon was set up, which prevented access to Borough Market for 10 days. As a consequence, many businesses (including market stallholders, bars and restaurants) were significantly impacted. While many did not suffer any physical damage to their buildings, contents or stock, the inability to trade led to an estimated loss of around £1.4m.

It took 26 days for the attack to be certified as an act of terrorism by HM Treasury, leaving policyholders in limbo at a time when their businesses were most affected. Once that certification came, there was more bad news for policyholders whose businesses had been interrupted through their customers, suppliers and staff being denied access to the market, but who had not actually suffered any physical damage to their property. Pool Re did not respond because their legislative remit currently does not extend to cover non damage business interruption. This meant that businesses might have been better off, had the attack not been certified as an act of terrorism.

In such circumstances, business interruption policies (which are subject to terrorism exclusions) may include extensions of cover for loss of profits which flow from denial of access, or the actions of authorities (such as the police) within the vicinity of the policyholder's premises.

Fortunately, there is good news for commercial policyholders and brokers on the horizon in the shape of the Counter Terrorism and Border Security Bill 2018, currently progressing through Parliament, which will address this.

£1.4m

While many did not suffer any physical damage to their buildings, contents or stock, the inability to trade led to an estimated loss of £1.4m after the London Bridge terroist attack.

TIME'S UP FOR DEFICIENT INDEMNITY PERIODS

AUTHOR:
HARRIET CONWAY
SME BUSINESS INSIGHT MANAGER, ALLIANZ

A spotlight was turned onto non-damage business interruption (BI) by 2017's terrorist attacks, which acted as a catalyst for the extension of Pool Re's cover, but for brokers and insurers there's still some work to be done bringing the issue of indemnity periods that are too short out of the shadows.

Businesses sometimes underestimate the time it can take to return to the trading position they were at prior to a loss. It's important to consider the length of indemnity period that will cater for this. The insurance industry is in a prime position to educate business owners on the dangers of taking an optimistic stance on the likelihood of being faced with disruption and the amount of time it would take for them to return to 'normal' and brokers are well placed to help with this. Using illustrations and case examples (such as those on the opposite page) can prove to be an effective way of demonstrating to businesses how operations like their own can end up in a situation where a lengthy indemnity period is needed.

The Salisbury Novichok attack in March, for instance, can serve as a case example of why 'Loss of Attraction' (LoA) is a worthwhile extension on insurance policies that incorporate business interruption and/or terrorism covers. Many businesses in the area saw a fall in visitor numbers of up to 80% and those who did have LoA cover may have been offered some relief. However, they were only just seeing signs of recovery three months on, as the duration limit of standard LoA indemnity periods was being reached, when another major incident, related to the original, was declared.[1]

The Novichok attack is an extreme example; on the next page are some more relatable examples that can be used to illustrate the complexity of business interruption.

Even better than using examples of problems faced by other businesses is to engage the services of crisis simulation providers so that all aspects of a business which are vulnerable to interruption can be identified. As an alternative for smaller businesses, there are business impact assessments templates readily available that can be used as part of business continuity planning.

A deficient indemnity period is just one form of underinsurance, which is a key topic to include in discussions with customers about business interruption and continuity planning.

In her January 2018 article, 'SMEs: Overbalancing and underinsured', Harriet delves further into the issue of underinsurance, including a look at 'average', valuations and additional expenditure during interruption.

READ THE FEATURE AT ALLIANZEBROKER.CO.UK/OVERBALANCINGSMES

1 "It's going to ruin our year": Salisbury business owners express fears over future after second novickok poisioning' (06/07/2018), Independent.co.uk

PUB/RESTAURANT

A major fire broke out in the kitchen resulting in the building and equipment being damaged by fire, smoke and water. Initial assessment of the damage indicated that all equipment needed replacing with indicative lead times of around six months. Added to this, the building required complete re-roofing due to severe heat damage.

The logistics involved in dealing with the equipment removal and subsequent replacement roof indicated an overall reinstatement time of about 14 to 15 months. In this case a maximum indemnity period of 12 months was insufficient. It's important for businesses to consider if maximum indemnity periods, of 24 months or more is necessary.

FACTORY/PRINTER (SUPPLY CHAIN FAILURE RESULTING IN LOSS OF BUSINESS)

The manufacturer of essential specialist machinery suffers a major fire and goes into administration. For its customers it becomes very challenging to find compatible spare parts to make repairs or replace worn-out components, and ultimately some of their machinery becomes unusable. While either trying to source the parts or acquiring new machinery, they're unable to produce to the usual capacity and fulfil orders. In this situation having a Suppliers' Extension to their BI policy may provide cover for losses arising directly from the suppliers' fire.

RETAILER WITH A 'HOLE-IN-THE-WALL' ATM

Overnight, the premises is subject to a 'ram-raid' attack on the ATM machine which caused extensive damage to the building. It will take at least eight weeks to restore the premises to a state from which the business can resume trading. The ATM itself may be out of action for longer so this highlights the need to think about every aspect of a business and what incidents might impact its revenue stream.

ASSESSING THE INTERRUPTION RISK

A broker asked BIBA's valuation provider QuestGates to help value a boutique hotel. It was a listed building set on an island in a trout fishing lake.

To assess the correct rebuilding cost and reinstatement time the valuers had to think outside the usual considerations and look at the cost of potentially having to drain the lake to access the ground source heating pump buried beneath and the need to add in the cost of hiring a materials ferry to enable reinstatement of the building, the sole access being via an iron footbridge.

BIG DATA. BIG RISKS. BIG LOSSES – CYBER BUSINESS INTERRUPTION

AUTHOR:
ILANA GILBERT
ASSOCIATE
DAC BEACHCROFT LLP

A cyber attack or operational IT failure can cause major disruption, with serious financial and reputational consequences.

Business interruption cover has largely been derived from property damage business interruption cover. However, when considering cyber risks there are fundamental differences.

One of the starkest differences is the lack of physical cause. In a cyber world it can be far more challenging to evidence a virtual cause and quantify losses. Underwriters and brokers need to consider carefully the language defining the cause of the disruption, its impact on the business and what can be done to mitigate it as this is of critical importance to claims handlers.

Another big difference is the duration of disruption and the required indemnity period, and how this relates to policy wordings. Business interruption wordings will typically apply a financial deductible or a time-based waiting period. Property business interruption indemnity periods factor in lengthy rebuild or repair times. Cyber events can hit an online retailer hard in a few hours. Typically large losses can occur in the first 6-12 hours following the incident. If the policy deductible has a similar time deductible, then the insured may find that the policy offers little or no indemnity.

Cyber business interruption claims are subject to adjustments for external factors, such as industry or market trends. If an online retail website goes down, the loss of sales will depend on the exact time of the outage. Certain holiday periods or promotional weekends can affect the business dramatically.

The definition of the indemnity period itself requires thought, particularly if there is an operational IT failure and any aggregation wording will be a key consideration.

Supply chain and contingent business interruption risk is challenging to write in the physical domain with a greater level of complexity in the cyber network infrastructure world. An incident at a major internet or cloud services provider, or a security flaw in a systemic software product, could result in a huge accumulation risk for the insurance industry.

Underwriters and brokers may need to consider whether they wish to offer reputational damage cover. Given the frequent coverage in the press, GDPR, and data security, a breach triggering a cyber business interruption loss can have an impact on both new and old customers.

Whilst actuarial developments will help insurers better understand cyber exposure, this needs to be reflected in the policy wordings and insurers will need to keep the scope of cover being offered under review.

BUSINESS CONTINUITY PLANNING FOR THE DIGITAL AGE

Currently, the list of things that might stop businesses trading is fairly small and can range from a lack of materials to connectivity problems and inaccessible premises. Could the technology we're introducing into the workplace make this list longer?

AUTHOR:
ANNEKE GRAHAM
ENGINEERING
UNDERWRITING
MANAGER,
ALLIANZ

The invention of the boring machine in 1774 marked the start of the era of mass production, which formed an integral part in the Industrial Revolution. Mass production meant that large amounts of product, all conforming to a certain standard, could be manufactured speedily and efficiently, but with the machinery that enabled this came risks, such as bodily entanglement and fires, and it created a new potential for disruption within a business and in supply chains.

Consider autonomous vehicles and shipping, which some fear will make many jobs redundant. The capability to self-drive is dependent on an array of technology, including cameras, motion sensors and GPS trackers, as well as the mechanical make-up of the engine, ancillary parts and fuel. This means that, in addition to the assortment of problems that can occur with non-autonomous vehicles, a fault with an element that permits safe self-driving becomes another potential cause of interruption as the vehicle is taken off the road. Arguably, the likelihood that a human driver calls into work sick is higher, but herein lies the debate: is technology creating more or fewer business interruption problems?

All sorts of businesses are becoming more dependent on machinery and computer technology for the everyday running of operations. As an example, some traditional retailers don't accept cash payments and aren't equipped to do so. If their card machines and/or cashless payment points are lost, damaged or go down due to connectivity or power supply issues, how much of their income would be lost during the downtime?

The insurance industry, and particularly brokers are well positioned to make business owners aware of how increasing their dependency on technology, for all its efficiencies and precision, might be making them more vulnerable to business interruption.

There's no doubt that more and more new types of insurance cover will emerge to accommodate the transition into the digital age, but the reassurance these can provide pale in comparison to a well thought-out business continuity plan that carefully considers the risks bundled in with new technology.

Brokers can add value by encouraging customers to bolster the resilience of their business by not taking all the technology available for granted. In addition to continuity planning, advise them to take all appropriate preventative measures too, such as regularly checking equipment for faults and disrepair, just like you would for a car, and keeping up-to-date on the latest emerging threats, such as cyber security vulnerabilities.

A SUPPLY CHAIN REACTION

Supply chains are core to the majority of businesses and effective supply chain management can offer companies a competitive advantage through increased output, tailored customer solutions and speed to market. However, where supply chains break down, this may cause significant business interruption, slowing down or completely halting normal operations.

AUTHOR:
PAUL BALLARD
LOSS CONTROL ENGINEERING MANAGER, ALLIANZ

Supply chain management is still a relatively new concept, reportedly first mentioned in 1982 by a consultant at the American technology firm, Booz Allen Hamilton.[1] Since then, it's evolved from a relatively simple exercise of controlling an end-to-end set of processes to a more integrated approach, employing predictive forecasting, automated KPI reporting and robotics. This is largely driven by changing customer expectations of faster lead times and more bespoke products. To meet such expectations, some companies rely on 'just-in-time' deliveries, where only the right quantity of parts is delivered, and solely when critically required in the production process.

This has the benefits of cost and storage reduction but can be a risky approach, placing a heavy reliance on suppliers, often to tight deadlines. This propulsion towards lean manufacturing is resulting in longer, more complex supply chains. What used to be a fairly siloed process has transformed into a global network of interconnected suppliers and manufacturers, each with their own supply and demand dependencies. This means that risks in one industry or country can have a ripple effect, passing through the chain and threatening business operations across different industries and even continents.

Causes of supply chain disruptions are wide-ranging; natural catastrophes, political violence and machinery breakdown can all cause a sudden 'chink' in the chain which has repercussions for businesses elsewhere in the network. More and more, supply chain disruption stems from a digital rather than a physical incident. With companies increasingly reliant on IT systems and data centres, it's important to consider how an IT outage could impact the ability to deliver products or supply services, plus lead to costs for resolving the issue. And there are further potential consequences of supply chain disruption, including loss of productivity, increased cost of working, customer complaints and regulatory investigations.

Insurance alone cannot eradicate the risks associated with supply chain disruption. Rather, businesses should look to further strengthen their resilience through adoption of supply chain risk management (SCRM). SCRM is about avoiding and managing the potential impact of events occurring at any point in the supply chain. Step 1 for a business is to identify supply chain risks which may present themselves, including those which could originate from both the main supplier site and from any secondary suppliers; these may include distribution difficulties or manufacturing delays. It's also important to consider any factors in the macro environment which could present a risk, such as those linked to the environment, natural disasters or political unrest. Once the risks are identified Step 2 is to assess and prioritise each risk, potentially using a risk register

approach. In Step 3, control measures are considered, where it may be possible to avoid, transfer or mitigate each individual risk. Step 4 involves putting in place an effective monitoring system. This may include undertaking periodic reviews, testing and post-incident analysis. Additionally it's a good idea for a business to review and validate its own and any key suppliers' business continuity plans.

Since many supply chains now belong to a wider ecosystem, it's increasingly important for a company to look beyond the 'Tier 1' supplier and familiarise themselves with their suppliers' supplier. According to a 2018 survey carried out by Deloitte, as many as 65% of procurement leaders have limited or no visibility beyond their Tier 1 suppliers.[2] Also prudent is to source alternative suppliers as a contingency and avoid single suppliers wherever possible. Those involved in business continuity planning (BCP) may choose to examine and test each link in their supply chain, considering possible failure points and planning for recovery should one section 'collapse'. Ensuring a robust BCP is in place and tackling problems early is key to mitigating the repercussions of supply chain disruption. The looming deadline of Brexit will undoubtedly bring new challenges to UK supply chains. There are fears that trade barriers may appear post-Brexit and a survey of 1,000 UK supply chain managers reported that 20% of UK companies involved in supply chains have struggled to secure contracts that run beyond March 2019.[3]

Technology is playing an increasingly significant role in supply chain management, meaning that companies can capture, analyse and interpret real-time data. Robotics are being used to improve productivity; delivery drones and self-driving vehicles are being explored for transporting goods and sensor data is being analysed to better estimate when machines may break down.

It's important to put measures in place to help protect a business in the event of a breakdown in the supply chain. A combination of business interruption insurance, familiarity with all elements of the value chain and effective SCRM can all put companies in a stronger position to recover quickly and repair their broken chain.

65%

According to a 2018 survey from Deloitte, as many as 65% of procurement leaders have limited or no visibility beyond their Tier 1 suppliers.[2]

1 https://www.bloomberg.com/research/stocks/private/person.asp?personId=8106015&privcapId=1080523
2 The Global Chief Procurement Officer Survey 2018 (Deloitte)
3 Chartered Institute of Procurement and Supply

WWW.BIBA.ORG.UK

BIBA GUIDES

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

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

Allianz Insurance plc
57 Ladymead, Guildford
Surrey GU1 1DB

DAC Beachcroft
3 Minster Court, Mincing Lane,
London EC3R 7DD

Produced by **SandisonPay**
01329 835135
www.sandisonpay.co.uk

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

- Security measures in today's world
- The Future of Motor Insurance
- Construction Risks and Opportunities
- The legal and regulatory aspects of marketing
- InsurTech
- The Broker's role in Claims