



TERRORISM INSURANCE GUIDE

British Insurance Brokers' Association



BIBA

POOL RE

REINSURING TERRORISM RISK





RT HON BEN WALLACE MP
Minister of State for Security
and Economic Crime



This new guide from BIBA and Pool Re will really help to raise the importance of terrorism insurance particularly for small and medium enterprises.

The threat of terrorism is ever present and evolving. The aim of Government's counter-terrorism strategy, CONTEST, is to reduce the risk to the UK, its citizens and interests, so that our people can go freely about their lives with confidence.

As part of our strategy we are working to better integrate with the private sector to protect our economic infrastructure, improve safety, security and resilience. This new guide on terrorism insurance will further our joint aims of improving resilience within UK businesses and its citizens.

We know that UK insurance brokers, with their close relations to businesses are well placed to help improve the financial resilience of SMEs in the face of potential attacks."



GRAEME TRUDGILL FCII
BIBA's Executive Director



The Counter-Terrorism and Border Security Act 2019 allows Pool Re to provide reinsurance cover to insurers in order to protect businesses that suffer losses as a result of acts of terrorism even though their premises have not been physically damaged.

BIBA was delighted to work with Pool Re, HM Treasury and Members of Parliament, including Neil Coyle MP whose constituency includes Borough Market which was badly affected by an attack in 2017, to bring this Act into being.

We know however, that there is a need to encourage more businesses to buy terrorism cover; currently fewer than 3% of SMEs take up any cover at all. This guide explains: the need for terrorism cover for businesses; what cover is available and how to arrange it; extensions including cyber insurance; resilience; claims; and other policies. We aim to enhance understanding among both insurance brokers and their business clients (whether they are operating from their own premises or as a tenant in a building). The simple checklist will also serve as a useful aide-memoire for businesses.

We hope this guide can help to improve the understanding and take-up of important terrorism insurance protection for UK businesses.”



POOL RE

JULIAN ENOIZI
Chief Executive, Pool Re



Pool Re was delighted to be asked to be a key contributor for this BIBA Terrorism Insurance Guide. We recognise the vital role insurance brokers play in ensuring commercial policyholders obtain the most appropriate insurance cover for their business. BIBA plays a pivotal role in this regard by creating and maintaining standards, promoting good practice and providing technical information and guidance.

Terrorism is a unique risk in many ways, not only by its very nature but crucially in the ability of terrorist groups to adapt and innovate. The practical effect of this is well illustrated by examining the attacks in Europe in recent years. Attacks have involved IED (improvised explosive device), knives, guns and latterly vehicles, and this in turn means insurance professionals need to keep up-to-date with the nature of the threat so they can design and sell insurance solutions that will respond accordingly.

Though Pool Re's remit is restricted to commercial property, the events of 9/11 highlighted that there are few classes of insurance that are not exposed to terrorism in some shape or form. Property, Liability, Accident and motor policies can all be exposed to terrorism losses and while some of these policies cover terrorism automatically, others do not. In the UK brokers selling commercial property policies need to consider advising their client to buy an additional terrorism policy, either from a Pool Re member insurer or from Lloyd's. Understandably clients want to understand why they should buy such additional cover and Pool Re is proud to support BIBA members in making the argument that there are few businesses that can afford not to buy terrorism cover.

We believe that this guide provides straightforward explanations of the issues surrounding terrorism, which we hope will help BIBA members to have informed and productive discussions with their clients."



CONTENTS

1. The **need** for **terrorism** insurance

- 1.1 Why is terrorism insurance so important?
- 1.2 Counter-Terrorism & Border Security Act 2019
- 1.3 Threat level and response
- 1.4 Incidents are not confined to major cities
- 1.5 Take-up of terrorism cover
- 1.6 Common objections to buying cover

2. What is **available** / how to arrange **cover**

- 2.1 Pool Re
- 2.2 Other insurance providers
- 2.3 Pool Re non-selection rule
- 2.4 Types of cover available
- 2.5 Non-conventional cover / Chemical, Biological, Radiological, Nuclear (CBRN)
- 2.6 Northern Ireland

3. **Extensions** to think about

- 3.1 Business interruption - extensions to cover
- 3.2 What about loss of attraction?

4. **Cyber**

- 4.1 Cyber terrorism property damage
- 4.2 Terrorism cover elements within specialist cyber insurance policies

5. **Resilience**

- 5.1 Pool Re - Vulnerability Self-Assessment Tool
- 5.2 Businesses continuity plans
- 5.3 Recognising the terrorism threat
- 5.4 Cyber terrorism resilience
- 5.5 Department for Transport Rental Vehicle Security Scheme
- 5.6 Security Considerations Assessment (SCA)

6. **Claims**

- 6.1 Pool Re claims process

7. **Other policies**

- 7.1 Motor insurance
- 7.2 Casualty/liability
- 7.3 Home insurance
- 7.4 Travel insurance
- 7.5 Different classes of insurance

8. **Customer checklist**

- 8.1 Customer checklist - key points to consider

9. **Glossary**

THE NEED FOR TERRORISM INSURANCE

AUTHOR | STEVE COATES ACII – CHIEF UNDERWRITING OFFICER, POOL REINSURANCE COMPANY LTD

1.1 Why is terrorism insurance so important?

Like many other catastrophe perils, a terrorism incident can disrupt or destroy a business so protecting the business with insurance is a sensible mitigation strategy.

However unlike natural catastrophes, terrorism manifests itself in a dynamic and constantly changing manner and is unpredictable not only in its frequency and severity but in its very nature. Evidence for this can be seen by examining the recent history of terrorism. Terrorist tactics and methodologies during the 1970 to 2000 period featured significant use of guns, bombs, hijackings and kidnappings, but since 2000 methodologies have also included attacks involving vehicles as weapons, knives, airplanes and chemical or biological compounds. Tomorrow's attacks could include cyber terrorism, drones and radiological isotopes.

Given the inherent unpredictability of terrorism, combined with its constant evolution, a business that does not buy terrorism insurance is vulnerable and that vulnerability will probably increase over time as terrorist methods evolve.

Some businesses may consider that it is more beneficial to save the additional premium needed to buy terrorism cover. Though this can be challenged as it seems illogical for those businesses to invariably buy cover for natural perils while leaving themselves vulnerable to something that is able to constantly change and is ultimately created to cause harm and disruption.

Do all commercial insurance policies exclude terrorism? No, many still provide some cover although commercial property policies invariably contain a terrorism exclusion.

By way of example: liability policies in the UK usually include terrorism but with a sub-limit applied above a certain level; motor personal injury sections include the cover to an unlimited extent but the damage element is sub-limited; and personal accident (PA) travel policies may include or exclude depending on the market segment.

Interestingly, reinsurance is no longer available from the global market on an unlimited basis for third party motor injury, so this risk now has to be reinsured to the Motor Insurers' Bureau (MIB). This is covered in Chapter 7.

POINTS TO CONSIDER

- Be mindful of the changing threat of terrorism and its unpredictability
- UK insurance policies vary greatly in relation to terrorism exclusions and the application of sub-limits

AUTHOR | BIBA

1.2 Counter-Terrorism & Border Security Act 2019



Sadly I know all too well about the devastating impact that a terrorist attack can have on a local community and its businesses. In 2017, eight innocent people were killed and many others injured in the appalling attack at London Bridge and Borough Market in my constituency. More than 150 businesses were affected and, due to the area being shut off for 10 days for the extensive police investigation, the cost to local employers was over £2 million.

I campaigned with BIBA to better protect communities and employers and I'm pleased we have a new Counter Terrorism and Border Security Act, which allows businesses to be covered for non-physical damage suffered through acts of terrorism.

Terrorism insurance will now not only help businesses get back on their feet in the event of an attack, it's also a vital tool in ensuring terrorists will fail in their efforts to disrupt how we live our lives and go about our work."

Neil Coyle MP



The Act that came into force in February 2019 resulted from terrorist events that occurred in recent years. In particular the incident at Borough Market in 2017 in which businesses that suffered no physical damage were still faced with financial loss as a result of denial of access.

Some insurers do cover non-damage business interruption (NDBI). However where business interruption (BI) cover was not effective because of the lack of physical damage, some providers did make ex-gratia claims payments to businesses that had bought Pool Re terrorism insurance. Subsequently, BIBA, along with Neil Coyle MP for Bermondsey and Old Southwark, raised concerns about the gap in terrorism insurance cover where no physical damage to the premises occurred.

At that time Pool Re, whose remit is governed by statute, could only respond to claims for material damage and / or business interruption following property damage. Subsequent campaigning brought into law the Act which allows Pool Re to provide cover for non-damage business interruption.

As a result, Pool Re members can, with relevant agreements, cede NDBI to Pool Re and offer the extension to cover, as long as the client's underlying commercial insurance policies reflect this. Importantly, Pool Re members may elect not to cede NDBI to Pool Re and retain for their own account – in other words they would still offer the cover, which may be higher or lower than cover that Pool Re is prepared to give, but not reinsure it to Pool Re. This cover can be added mid-term (provided a premium is paid).

The scope of reinsurance cover offered by Pool Re for NDBI is non-damage denial of access and/or non-damage loss of attraction. Further details of the cover can be found in Chapter 3.

Pool Re anticipates those insurer members who intend ceding NDBI will sign up to offer this new cover through March and April 2019. Cover should then be available later in the year.

POINTS TO CONSIDER

- Ask if insurers have entered into the new agreement allowing them to cede NDBI to Pool Re
- NDBI cover can be added mid-term

AUTHOR | OFFICIALS FROM THE PROTECTIVE SECURITY SECTION – OFFICE FOR SECURITY AND COUNTER TERRORISM

1.3 Threat level and response

There are five levels of threat:

CRITICAL	an attack is expected imminently
SEVERE	an attack is highly likely
SUBSTANTIAL	an attack is a strong possibility
MODERATE	an attack is possible but not likely
LOW	an attack is unlikely

The level is set by the Joint Terrorism Analysis Centre and the Security Service (MI5).

Terrorism incidents can occur at any time or place without warning.

In addition to pursuing terrorists and preventing others from becoming violent extremists the police service carries out daily activities to help increase the protection and security of our citizens, public institutions, critical national infrastructure, businesses and places, including those who are potential terrorist targets.

This concerted effort, which includes highly visible, covert, armed or technical methods, is aimed at protecting the public from the threat of terrorism, boosting the security of key sites, reassuring businesses, workers and visitors so they can go about their daily lives, and making the UK a hostile environment for terrorists to operate in. Security measures and activities are constantly reviewed to reflect where the threats exist and the level of threat the UK is facing.



Key actions to boost protective security include carrying out high visibility patrols in and around key areas in the country to reassure the public and to disrupt terrorist planning, increased physical measures to keep the public safe, protecting our critical national infrastructure to help ensure the country's communications, energy and transport networks can operate more securely.

Through Government's 'UK Protect' publications business and community vigilance is encouraged through awareness and information campaigns supported by the delivery of regional events to provide key advice to businesses, public sector and other institutions. The ACT (Action Counters Terrorism) suite of products has also been developed to deliver further awareness to businesses in relation to protective security.

To reinforce this approach, See, Check and Notify (SCaN) has been developed in partnership with colleagues from the Centre for the Protection of National Infrastructure (CPNI), as a cohesive package that helps an organisation, through the use of its own resources, to independently deliver a sustained hostile environment to disrupt those with malicious intent. It provides businesses with the knowledge and skills to achieve the desired effect. The Communications, CCTV, 'For All' and 'Customer Facing packages' help those responsible for security managers to develop capabilities to use, co-ordinate and deploy.

Businesses can find out more about the ScaN package and how to access the training by contacting their local Counter Terrorism Security Advisers via the Gov.uk website section on 'working with counter terrorism security advisers'

www.gov.uk/government/publications/counter-terrorism-support-for-businesses-and-communities/working-with-counter-terrorism-security-advisers

Counter-terrorism policing and local forces work throughout the year with event organisers, partners and commercial organisations across the country to give advice and guidance on safety and security measures, taking into account any specific intelligence and the wider threat.

More information on what to look out for and how to contact police can be found at www.gov.uk/government/organisations/national-counter-terrorism-security-office

Whilst further specialist security advice is available from the NaCTSO website, which also provides access to the National Stakeholder Menu of Tactical Options. This document outlines a set of options which can be used by the private sector and security industry to enhance their security posture at times of raised terrorism threat levels or in response to a terrorist incident. They can be employed independently or in support of the police service's 'National Menu of Counter Terrorism Tactical Options'. The document has been developed with the assistance and guidance of a number of security experts within the private sector.

Future measures

By 2021 and funded by Pool Re, Counter Terrorism Policing expect to deliver a new and innovative Information Sharing Platform (ISP) which will help deliver on the commitments in the government's counter-terrorism strategy, CONTEST. It will increase the UK's ability to tackle terrorism and also enable business, especially SMEs, to access timely and accurate information on the terrorism threat which ordinarily would be classified or costly.

The ISP increases risk awareness and mitigation, against the persistent threat of terrorism and will:

- Provide credible insights on risk mitigation and counter-terrorism best practice
- Send prompt messaging and authoritative advice in the event of a terrorist attack
- Allow personnel to develop their own counter-terrorism capacity through accredited online training
- Create professional and public forums in which best practice and ideas can be shared
- Issue calls to action against demography, geography, business and professions and
- Provide wider access to preparedness information, only currently available through restricted channels.

POINTS TO CONSIDER

- Look at the various government websites for security information
- Be aware of changes in threat levels and these websites:

CPNI - www.cpni.gov.uk

NaCTSO - www.gov.uk/government/organisations/national-counter-terrorism-security-office

Action Counters Terrorism - www.gov.uk/ACT

AUTHOR | BIBA

1.4 Incidents are not confined to major cities

When considering terrorism events within the UK the focus has tended to be on attacks that have taken place in London and other major cities, including, but not limited to:

- › **June 2007** - Glasgow Airport incident
- › **March 2017** – Westminster Bridge incident
- › **May 2017** - Manchester Arena incident
- › **June 2017** – London Borough Market incident
- › **June 2017** – London Finsbury Park Mosque incident
- › **September 2017** – London Parsons Green incident

However it is important to consider incidents that have occurred out of urban areas in recent times, including:

- › **February 2014** - New IRA parcel bombs to locations in Oxford, Brighton, Slough, Aldershot, Canterbury, Reading, and Chatham
- › **June 2016** - Murder of Jo Cox MP in Birstall, West Yorkshire
- › **March and June 2016** – Novichok poisonings in Salisbury and Amesbury, Wiltshire (although neither were designated as a terrorist incident)

Pool Re highlight the threats to the UK from Daesh, Northern Ireland related terrorism (NIRT) and Extreme Right Wing activists and they also highlight as likely targets: police, military and government personnel as well as crowded places associated with iconic sites and the transport sector.

When reviewing clients' exposures to the terrorism threat it may be appropriate to consider the impact to their business of a terrorism event at client's premises or in the vicinity of their premises.

While Pool Re (and other) cover is available in England, Scotland and Wales, the handling of property damage and business interruption losses in Northern Ireland is somewhat different due to historical issues. Terrorism cover is generally excluded from commercial property and business interruption policies. See section 2.6.

In the event of an incident being declared as of a terrorist nature by the Chief Constable for the Police Service for Northern Ireland, then compensation may be available from the Northern Ireland office in accordance with the Criminal Damage (Compensation) (Northern Ireland) Order 1977.

Please see the Guide for Criminal Damage Compensation in Northern Ireland - www.nidirect.gov.uk/sites/default/files/publications/guide-to-criminal-damage-compensation-northern-ireland.pdf

POINTS TO CONSIDER

- › Terrorism cover is a consideration wherever a business is situated not just in major cities

AUTHOR | KEVIN HANCOCK ACII – CHARTERED INSURANCE BROKER, MANAGING DIRECTOR, YUTREE INSURANCE LTD

1.5 Take-up of terrorism cover

In the current climate it would be appropriate for businesses to discuss their terrorism insurance requirements as part of their insurance portfolio. Despite the current threat level of international terrorism being ‘severe’ in the UK, this cover is rarely bought by SMEs. This heightens their vulnerability to financial loss.

There are a number of possible reasons for this that could be overcome by industry collaboration for example through more package products with the option for terrorism cover being available via broker software houses.

As well as Pool Re, there are open market alternatives for terrorism cover. These differentiate themselves by offering first-loss sums insured, selective cover and cover for overseas exposures that Pool Re cannot accommodate.

As indicated elsewhere in this guide Pool Re cover now includes non-damage business interruption as a result of a terrorism incident.

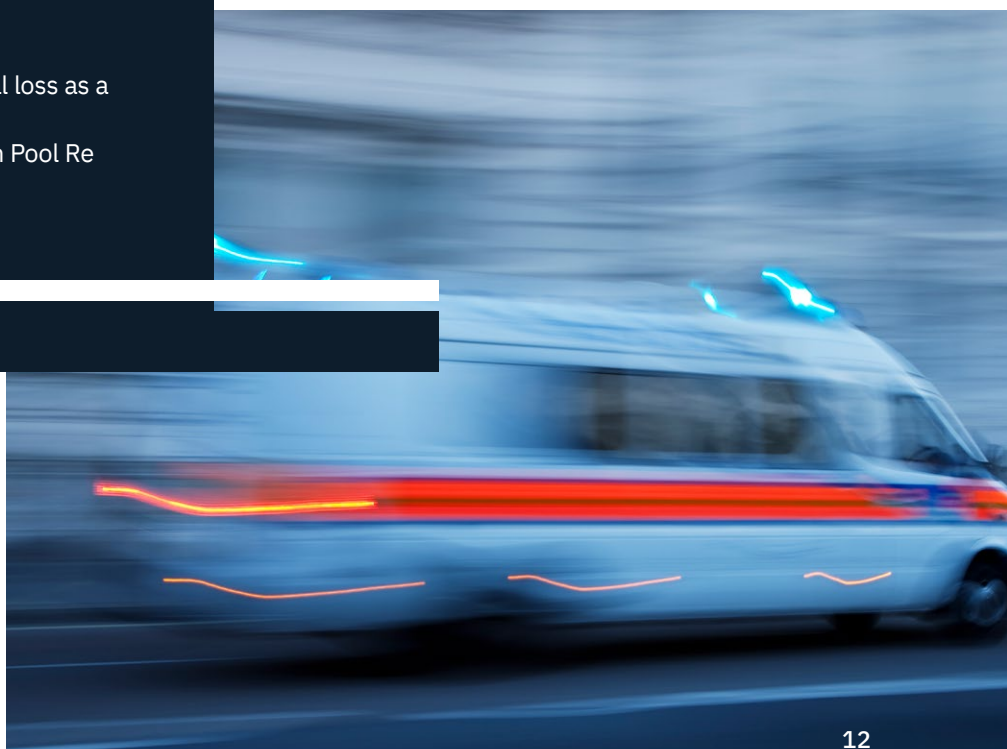
There will also be some differences between Pool Re members, for example in the treatment of CBRN events that may need wider consideration.

Finally, there will also be potential pricing differences and fluctuations in the wider terrorism insurance market. Pool Re’s terms are fixed according to the rating area while other insurers may have differential rating depending upon their capacity, appetite and demand for cover in a particular area. Some new innovations in cover include damage caused during the containment, control or suppression of an act of terrorism; looting post loss and alternative accommodation for up to 25% of the total insured value.

Small brokers are often the first port of call for SMEs and when discussing cover with clients it might be a consideration to examine their exposure to terrorism risk and explain the cover available and its extent.

POINTS TO CONSIDER

- The vulnerability of SMEs to financial loss as a result of terrorism
- The availability of options other than Pool Re





AUTHOR | STEVE COATES ACII – CHIEF UNDERWRITING OFFICER, POOL REINSURANCE COMPANY LTD

1.6 Common objections to buying cover

Prior to the IRA mainland campaign in the '80s and '90s, culminating in the Baltic Exchange bomb in 1992, insurance policies in the UK made no mention of terrorism and cover was automatically included within the fire and explosion perils. Pricing tariffs made no explicit provision for terrorism and no underwriting criteria were applied so everyone who bought property coverage was also covered for damage caused by terrorists.

That changed in 1993 when terrorism exclusions were applied to property policies in England, Scotland and Wales, and cover needed to be separately requested from the insurer who could then reinsure it to the newly established Pool Re. This effectively created a new type of insurance that had to be sold and priced separately. Inevitably this meant that while many businesses elected to buy this coverage, a larger number did not and that remains the case today.

The cost of terrorism cover can be a barrier to some businesses but the latest Pool Re Underwriting Manual includes a number of discounts not previously available. Moreover the basis of rating SMEs (with Material Damage (MD) sums insured below £2m) makes cover for these policyholders much more competitive. By way of example the reinsurance charge for an SME with a £500,000 MD sum insured, and based in Zone C or D, would be £30. Pool Re members may adjust this premium but the cost remains affordable for many.

POINTS TO CONSIDER

Objections to buying might include:

- › Price
- › Lack of awareness
- › Apathy and attitude: “It won’t happen to me”
- › Acceptance of risk
- › Self-insurance
- › Time it takes to get a quote
- › Policies limited in non-damage business interruption extensions

WHAT IS AVAILABLE / HOW TO ARRANGE COVER

AUTHOR | STEVE COATES ACII – CHIEF UNDERWRITING OFFICER, POOL REINSURANCE COMPANY LTD

2.1 Pool Re

BACKGROUND

For commercial policyholders in Great Britain, terrorism is most frequently purchased alongside their property policy and from the same insurer. Nearly all insurers who offer property cover in GB are members of Pool Re, which allows them to offer terrorism cover that is ultimately supported by this reinsurance scheme.

Pool Reinsurance Ltd was established in 1993 as a response to the market failure that was triggered by the bombing of the Baltic Exchange in London. Pool Re is an industry mutual, in that it is owned by its members (UK property insurers), but is backed by a loan agreement from HM Treasury, thereby forming a private sector solution to a public policy objective. This means it can offer affordable coverage to everyone who wishes to purchase cover, without being constrained by solvency or capital requirements.

Membership of Pool Re is open to any UK authorised insurer, whether they are an insurance company, Lloyd's syndicate or captive entity.

However once an insurer joins Pool Re, it must cede all eligible terrorism risks to the scheme and cannot retain any for its own account, beyond the retention under the scheme. Members of Pool Re must offer terrorism cover to any client who requests it as part of their commercial property policy. Each Pool Re member is allocated a retention, based on the amount of premium ceded, beyond which they can recover the cost of terrorism claims they receive.

Pool Re members can cede any eligible property risk to Pool Re. This includes any risk classed as commercial property or residential property in commercial ownership. Risks must be situated within England, Scotland or Wales and the scheme cannot accept risks written as marine, aviation, motor or casualty. Pool Re provides material damage and business interruption covers or related types of policy such as contract works, which for regulatory purposes is considered to be property.



RELATIONSHIP WITH PROPERTY POLICY

Pool Re only offers reinsurance for terrorism where it is written back to back with a property (or construction) policy. Terrorism written in isolation is not eligible for cession.

There are a number of reasons for this:

- The material damage/business interruption (MD/BI) and terrorism cover are intended to be back to back. This means the exclusion wording on the MD/BI policy uses the same definitions as the terrorism policy, thereby removing gaps in cover. If an event is certified as an Act of Terrorism it is then excluded under the MD/BI policy and falls to be considered under the terrorism extension. If it is not certified then it cannot be terrorism and should be considered a fire, explosion or malicious damage claim under the MD/BI. This is important when comparing cover with that provided by terrorism written separately or within political violence policies. Some of these say they will extend cover to sabotage, which may be helpful elsewhere in the world, but in the UK sabotage is either malicious damage or arson, and this is included in property policies, or if certified as terrorism then it becomes a terrorism claim.
- The terrorism cover is effectively an extension of the MD/BI policy and mirrors the terms and conditions. This means that sums insured and limits are automatically carried through as are conditions around claims handling.
- There can be no selection between the property policy and the terrorism and the interest, limits and deductibles can be seen to be consistent.

SCOPE AND EXTENT OF COVER

Terrorism cover provided by Pool Re members is very wide and extends to perils not typically covered by property policies. The cover is effectively 'All-Risks' with the only exclusions being war and related risks and certain cyber causes. This means damage caused by chemical, biological, radiological and nuclear (CBRN) causes is included if certified as terrorist in nature. Claims caused by CBRN perils are invariably excluded not only by property policies, but also other terrorism products although small sub-limits are sometimes available.

Furthermore, damage to tangible property caused by remote digital interference, or cyber-terrorism, is also now included. Importantly both CBRN and cyber-terrorism are covered to the full extent of the property sums insured or limits. Given terrorist groups aspire to deploy both of these potential attack vectors, the availability of cover to meet this threat is important.

As highlighted above, Pool Re members can offer terrorism cover to the full extent of all and every policy within their portfolio. Unlike some of the other global terrorism schemes, there is no financial limit to the reinsurance protection offered by Pool Re and this means its members are not constrained by eroding aggregate limits or geographical restrictions/limits. The unlimited nature of the loan guarantee from HM Treasury means every business in England, Scotland and Wales can purchase terrorism cover to the full extent of their financial needs.

POINTS TO CONSIDER

- Membership of Pool Re is open to any UK authorised insurer
- Insurers and clients must cede all eligible terrorism insurance risks to the scheme
- Great Britain only
- Pool Re cover provides material damage and business interruption
- Pool Re terrorism terms and conditions are a mirror of your commercial policy, however the scope of Pool Re terrorism cover should always be wider, and is effectively 'All-Risks' with only two exclusions; war and cyber (although the latter now contains a buy-back proviso). Therefore CBRN is included and, since April 2018 so is remote digital interference

AUTHOR | GARY BARLOW – TERRORISM UNDERWRITING MANAGER, NMU (SPECIALTY) LTD

2.2 Other insurance providers

Modern terrorist attacks (such as lone-wolf perpetrators) may not result in catastrophic property losses but they can still result in significant financial consequences for local businesses. Many such financial losses remain uninsured in the market.

The provision of cover for non-damage terrorist acts is essential for certain businesses in the current climate, especially those that are reliant on public footfall and custom, such as high street retail, hospitality and entertainment industries.

However, simply ensuring that cover includes non-damage denial of access may not go far enough to protect another real financial threat to business – loss of attraction.

Though it is much easier now than ever before to obtain non-damage denial of access cover, it still proves to be a challenge to ensure the longer term financial consequences are insured. This is where critical non-damage loss of attraction cover may be needed. After the incident is declared over, and the police cordons have been lifted, what about the weeks and months that follow, where public footfall declines and the business continues to suffer as a consequence?

Aside from addressing the non-damage terrorism threat, there are some very real and tangible benefits of a standalone terrorism product. Some policies may have a broader definition of what constitutes a terrorist act and will respond without the need for Government to certify the trigger as an Act of Terrorism.

Some may allow freedom to be selective on which properties are insured without breaching adverse selection rules, and others provide the ability to insure a portfolio on a first loss basis up to an agreed limit.

Some providers can cover risks overseas (including Northern Ireland – not covered by Pool Re.)

The standalone market cannot always address the full spectrum of concerns for every type of business (e.g. where perhaps Pool Re's ability to better cater for nuclear exposure could be a client's priority consideration). However the ever changing nature and focus of modern day terrorist attacks surely suggests that the alternative benefits of choice and flexibility the standalone market offers cannot be ignored.

POINTS TO CONSIDER

- › Loss of attraction might be valuable for some clients and not for others
- › Alternative providers can cover risks outside of GB



AUTHOR | STEVE COATES ACII – CHIEF UNDERWRITING OFFICER, POOL REINSURANCE COMPANY LTD

2.3 Pool Re non-selection rule

There are two key foundation stones of the Pool Re scheme. Firstly, both Pool Re, and by extension its members, must accept all eligible risks for terrorism cover and cannot decline an otherwise eligible risk.

The quid pro quo for that is that both members of Pool Re and their policyholders, must insure all of their risks through Pool Re. For policyholders this is ‘all or nothing’ and means that if they have a portfolio of, say 10 properties, they can either insure all 10 for terrorism, or none at all.

This is a fundamental feature of Pool Re and has been in place since 1993 and effectively means that the mutual fund cannot be selected against and be only exposed to high risk terrorism exposures. Where policyholders do wish to select and only insure certain locations, this option is available in the alternative market.

POINTS TO CONSIDER

- › Pool Re and its members must accept all eligible terrorism risks
- › Policyholders must ensure that all of their portfolio is insured through Pool Re irrespective of whether it is insured through one or more Pool Re insurers
- › If a policyholder wishes to only insure certain of its locations against terrorism or if it is not eligible for Pool Re, alternative markets are available



AUTHOR | STEVE COATES ACII – CHIEF UNDERWRITING OFFICER, POOL REINSURANCE COMPANY LTD

2.4 Types of cover available

Many types of policy that are broadly classified as property can be ceded to Pool Re. The principal types of coverage will be considered:

Material Damage – this is the most common coverage sought from Pool Re members and will most commonly extend to buildings (including tenants improvements), machinery/plant and contents, and stock. It can also incorporate computers, engineering plant, contract works (see CAR and EAR comments below), transport assets (e.g. trains), onshore energy (where insured on a property basis) and goods in transit (where insured on a property basis). Premiums are calculated in the same way as for the underlying coverage, by applying a rate to the total insured value. Cover extends to include any extensions granted within the material damage policy, provided they involve damage that occurs in England, Scotland or Wales.

Business Interruption (BI) – most BI terrorism covers are based on the standard revenue, profit, fees, income or increased costs of working basis. The scheme can also accept advanced covers, flexible basis, delayed start-up (DSU) and also time element (US style wordings). Maximum indemnity periods are available to the policyholder's requirements even if these extend to 5 or 10 years, and a commensurate premium is paid. Again premiums are based on similar principles to the underlying BI policy. Importantly BI extensions will also include terrorism cover if selected. This includes any damage based covers such as customers, suppliers, utilities and third party locations.

Construction - Construction All Risks (CAR) and Erection All Risks (EAR) – these can include contract or engineering works, contract plant and BI covers such as DSU, Additional Increased Cost of Working (AICOW), fines/penalties or advanced covers. Covers can be either annual or project policies. Typical risks insured via Pool Re include large infrastructure projects; large construction projects such as airports, skyscrapers, tunnels and roads; building redevelopments; new retail, warehousing, manufacturing; and housing/flat developments. Rating is either on annual contract turnover or project value, but as terrorism policies cannot be written for more than 12 months such project values must be apportioned annually.

Engineering – where engineering policies include damage caused by fire or explosion (not boiler or sudden/unforeseen), they can also be extended to include terrorism. Examples of risks written on this basis are computers, renewable energy and EAR type risks.

Contingency – until January 2019, risks classed as contingency could be ceded to Pool Re by its members. Typically this consisted of cancellation/non-appearance type exposures where terrorism was a peril that needed to be included. Risks included sporting events, concerts and tours. However such risks are now retained by the market, at its request as it is considered by all in this market that it has sufficient capacity without the benefit of reinsurance from Pool Re. However should such exposures be written on a property form, they can still be ceded to Pool Re.

POINTS TO CONSIDER

- All of a client's policy exposure must be ceded to Pool Re
- Some risk types e.g. contingency can be covered by Pool Re if written as a property class

AUTHOR | STEVE COATES ACII – CHIEF UNDERWRITING OFFICER, POOL REINSURANCE COMPANY LTD

2.5 Non – Conventional Cover/Chemical, Biological, Radiological, Nuclear

At its inception in 1993, the Pool Re scheme was restricted to terrorism damage caused by fire or explosion. In the aftermath of the 9/11 New York World Trade Center attack, cover was extended to ‘All-Risks’ which importantly did not exclude damage involving CBRN materials. The inclusion of CBRN coverage was important for a number of reasons.

- Property policies invariably exclude claims involving CBRN perils.
- The unprecedented nature of 9/11 indicated future terrorist attack vectors could include CBRN.
- Terrorist groups would use CBRN materials if they could acquire them. This can be seen from the widespread use of chemical weapons in Iraq and Syria by various groups including DAESH.
- A terrorist event using CBRN in the UK would be both unprecedented and potentially cause significant harm to both business and society.

The disruption that a very small amount of a toxic chemical agent could cause was illustrated with the tragic event in Salisbury during 2018. This not only caused a loss of income to businesses which were either within, or in close proximity to, one of the cordons, but also caused economic damage to a wider area in and around Salisbury.

While this particular event was not caused by an act of terrorism, it would be naïve to think such groups might not aspire to deliver an attack in the future using more accessible materials than the military grade agent used in Salisbury.

On the basis that commercial property policies exclude CBRN risks, the fact the terrorism extension will include such risks is a real benefit to policyholders and is the main aspect of cover where terrorism cover is not back to back with the property policy. In joining Pool Re, an insurer member undertakes to offer CBRN cover within their terrorism extension and cannot unilaterally decide not to offer this cover.

The inclusion of CBRN cover means there are several practical differences in how claims would be handled.

These are;

1. Both property and terrorism covers are triggered by damage and in 2019, are invariably written either on an ‘All-Risks’ basis or with accidental damage included as a peril. However, unlike the property policy, the terrorism cover will not have a general exclusion of radioactive contamination and nor within the MD/BI sections will it have a contamination exclusion. This means the scope of ‘damage’ is very wide.
2. As property policies have never covered CBRN (apart from very niche pooling of nuclear risks) there is little relevant precedent as to how the courts would apply the concept of damage to contamination claims. That said some general principles have historically been laid down that could help apply the cover. These include the broad concept of damage not being a temporary state of affairs and that contamination must in some way change the property it is alleged to have damaged. So there must be a difference between a radioactive isotope affecting both the fabric of a building and potentially the ventilation systems, and an infectious agent in the atmosphere that will dissipate naturally very quickly.

3. The concept of contamination brings with it a number of potential new or different heads of claim. The first that might be of concern is debris removal, which though a routine aspect of many fire and explosion claims, is complicated enormously when the debris itself is contaminated and potentially dangerous. Property insurers do have experience of this through clearing buildings with asbestos within them, but this would be nothing like clearing a building that had been contaminated with something like Caesium 137, an isotope that remains highly toxic for more than 30 years. Clearly having to knock the building down, clear the debris and rebuild is one scenario but in many others the building or property can be either cleaned up or decontaminated. However this in itself may be a very specialist job that few companies can undertake, and to clean to an acceptable standard such that people can use the building safely, might take some time. Moreover deciding to what level a clean-up must be done may not be the same as the level where the public will happily use the building again. The anthrax attacks (Amerithrax incident) in the US in 2001 illustrates this.

4. One of the key factors in any CBRN contamination incident would be the nature of the agent/ isotope/compound used. If it is complicated, toxic and durable any clean up or decontamination will be governed by the resources available to undertake the work. If many buildings are affected simultaneously then the clean-up may take a very long time.

The Pool Re scheme provides CBRN cover to the full extent of the policy sums insured or limits without restriction, provided it is a certified act of terrorism. This is one of the key differentiators between the UK terrorism scheme and many others around the world, where only France and Spain enjoy a similar level of cover. Moreover terrorism cover provided in the alternative market will not provide such unrestricted cover, if any at all.

POINTS TO CONSIDER

- Contamination and debris removal require serious consideration in relation to adequacy of indemnity periods
- CBRN cover is only available from the Pool Re offering

AUTHOR | COMPENSATION SERVICES – DEPARTMENT OF JUSTICE FOR NORTHERN IRELAND

2.6 Northern Ireland

The Criminal Damage (Compensation) (Northern Ireland) Order was introduced in 1977 in response to the escalating and sustained terrorist campaign in the 1970s which included attacks on the commercial heart of our towns and cities in Northern Ireland, resulting in an increasing number of high value claims. In addition, as a society in conflict there was a level of serious public disorder on our streets, leading to damage to both commercial and private property on a significant scale.

As a result of this terrorist campaign, many in the insurance industry withdrew from the Northern Ireland insurance market completely or refused to provide cover for riot and terrorist related damage. The insurance industry argued that the premiums they would need to levy on customers would be too high for them to bear and that it would not be financially viable for the industry to cover such high risk. The Government therefore stepped in effectively to underwrite the insurance industry by introducing a legislative scheme funded by the taxpayer, the purpose of which was to enable the victim to restore their property to its pre-incident condition.

The 1977 Order came into operation on 1 April 1978 and provides a right to claim compensation for loss suffered as a result of malicious or wanton damage to agricultural property and, in the case of other property, as a result of damage caused by an unlawful assembly of three or more persons or by a terrorist act. Although the Order was extended in 2009 to include cover to properties exempt from rates and used for or made available for charitable purposes, this is the first time since 1977 that the legislation has been comprehensively reviewed.

The fundamental purpose of the Criminal Damage Order is to reinstate victims of criminal damage to the position that they were in immediately prior to the incident which gave rise to their claim. The Criminal Damage Order provides compensation for damage resulting from terrorism. It also provides compensation for agricultural damage and loss. Compensation is not payable for damage of £200 or less. If compensation is payable, a statutory deduction (currently £200) is made from the claim.

The Criminal Damage Scheme in Northern Ireland is funded from the Northern Ireland Block Grant.

POINTS TO CONSIDER

- › In the same way that there are alternative offerings available in the market to Pool Re, there are also insurance solutions for businesses in Northern Ireland for the shortfall in compensation payable under the Criminal Damage (Compensation) (Northern Ireland) Order 1977



EXTENSIONS TO THINK ABOUT

AUTHOR | STEVE COATES ACII – CHIEF UNDERWRITING OFFICER, POOL REINSURANCE COMPANY LTD

3.1 Business Interruption – extensions to cover

Most terrorism schemes and policies were created primarily to respond to losses triggered by damage to property as that was the principal attack method that drove the global reinsurance market to exclude cover from property policies. However, terrorist tactics have moved on and groups such as DAESH have focused on attacks using guns, knives, vehicles and small explosive devices, as distinct from macro attacks using larger bombs or aircraft.

Business Interruption (BI) policies traditionally followed property policies in that they required material damage to have occurred to the insured property in order for the BI cover to trigger. However, since the 1980s, BI policies have been extended more regularly to cover a range of other contingencies, most of which are still triggered by damage but many now fall within the broad definition of ‘non-damage’ covers.

Recent attacks in UK and Europe have highlighted the terrorism gap, which is the effect of most property policies covering non-damage BI but excluding terrorism, and most commonly available terrorism policies being restricted to damage.



To examine the types of coverage that are required to meet the contemporary threat, we can start by looking at some of the extensions typically found in BI policies. These can be sub-divided into damage based extensions, and non-damage extensions.

DAMAGE EXTENSIONS

- **Suppliers & customers** – this is a common extension to most BI policies and will indemnify the insured for business interruption resulting from damage (as insured by the policy) that happens at the premises of one of their suppliers or customers. It is usual for a sub-limit to apply. If terrorism cover is bought as an extension of the MD/BI policy from a Pool Re member, and the BI policy has a suppliers or customers extension, it will automatically extend to damage (certified as terrorist in nature) occurring at these premises, subject to the same sub-limit. Importantly the scope of such terrorism cover will mirror that provided at the insured’s premises, thus including CBRN.
- **Public utilities** – another common extension which covers the insured for BI caused by damage at the premises of any gas, water, electricity or telecoms provider. A sub-limit may apply. Again, terrorism cover bought from a Pool Re member will then include damage at public utilities.
- **Third party storage sites/ contract sites** – where an insured stores property at third party locations, or carries out activities on a contract site, and damage is caused to its property at such sites, BI cover will be provided. A sub-limit will apply. Where terrorism cover has been purchased from a Pool Re member, it will extend to these sites.
- **Denial of access** – where damage in the vicinity of an insured’s premises prevents or hinders access to the insured’s premises, any resulting BI can be covered. A sub-limit will apply and/or a restricted indemnity period. A franchise of 24 or 48 hours may also occasionally apply. Terrorism from Pool Re members will again cover this extension as long as covered in the underlying BI policy, although in respect of damage triggered by remote digital means (cyber-terrorism) damage must have occurred within a one mile radius of an insured’s own premises.
- **Loss of attraction** – BI policies can be extended to cover losses resulting from a reduction in footfall, attractiveness or custom due to damage in the vicinity of the insured’s premises. Such extensions invariably contain either a sub-limit or inner indemnity period, and may also have an excess or franchise period. Where a Pool Re member provides terrorism cover by Pool Re it can be extended to include loss of attraction provided the underlying policy provides such coverage too.

NON-DAMAGE EXTENSIONS

- **Denial of access** – this is slightly different to the damage based denial of access cover. The trigger for non-damage denial of access is where access to or use of the insured’s premises is prevented or impaired due to the actions of either the police or any competent/statutory authority. The event triggering the police action must usually be either within the vicinity of the insured’s premises or a specified radius (usually one mile). Cover will either be sub-limited or have an inner indemnity period of around three months. A 24 or 48 hour franchise may also apply. Not all BI policies include non-damage denial of access, so for terrorism cover to apply the BI policy must be extended too. See following section on non damage terrorism.
- **Specified or notifiable diseases** – this is a fairly common extension and will cover the insured for BI due to the occurrence of certain diseases (sometimes listed as ‘specified’ or just defined as ‘notifiable’) at the insured’s premises or within a specified radius. Cover is usually sub-limited or an inner indemnity period applies. Pool Re reinsurance could respond to a denial of access caused by a terrorist deploying a disease or pathogen.
- **Murder/suicide/drains/vermin** – there is a range of other extensions commonly provided and which involve BI caused by the stated contingency at the insured’s premises or within a specified radius. Some of these are relevant to terrorism and commented upon later.

- › **Loss of attraction** – although most loss of attraction extensions are triggered by damage, they can occasionally extend to other contingencies. By way of example, pollution of sea beaches nearby is an extension seen within many hotel policies. Non-damage loss of attraction is not commonly available although hybrid or bespoke extensions are provided to corporate clients.

- › Since April 2018, terrorism cover reinsured by Pool Re has extended to include damage triggered by remote digital interference (cyber-terrorism), but no such coverage will be provided within the non-damage BI cover Pool Re offer, which will therefore exclude any losses triggered by remote digital means.

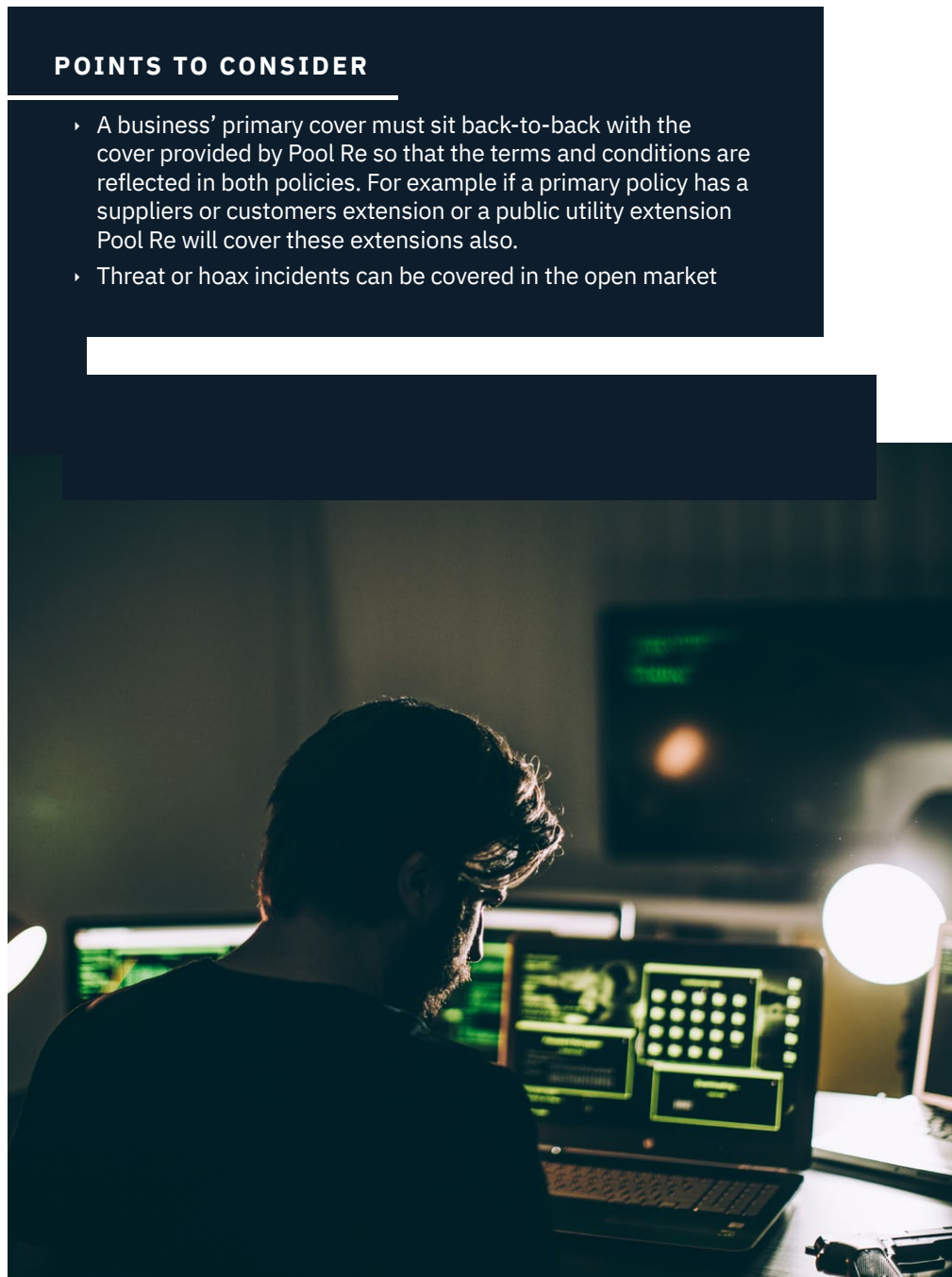
- › In addition a number of Lloyd’s managing agents have launched terrorism propositions that extend to include BI caused by non-damage events. Cover may be slightly different to Pool Re in that whilst CBRN may not be included, other threat or hoax type events will be and cover may also apply to other malicious acts not capable of certification as terrorism.

NON-DAMAGE TERRORISM

- › Until recently terrorism policies did not extend to include non-damage events (such as what occurred at London Bridge in May 2017). Since then the market has been working on closing the gap in coverage so policyholders can buy cover that meets the modern threat.
- › Government stated in early 2018 that it would amend legislation to allow Pool Re to offer non-damage cover and the Counter-Terrorism and Border Security Act received Royal Assent in February 2019. Pool Re members are now able to offer non-damage BI terrorism cover within England, Scotland and Wales, to the full extent of the limits and terms in the underlying BI extension. This means an event like London Bridge, where the loss and interruption did not result from damage, could be covered.
- › The scope of reinsurance coverage offered by Pool Re is non-damage denial of access and loss of attraction, provided such cover is provided in the underlying BI policy. Cover includes CBRN with disease type incidents not excluded provided they are certified as terrorist in nature.

POINTS TO CONSIDER

- › A business’ primary cover must sit back-to-back with the cover provided by Pool Re so that the terms and conditions are reflected in both policies. For example if a primary policy has a suppliers or customers extension or a public utility extension Pool Re will cover these extensions also.
- › Threat or hoax incidents can be covered in the open market



AUTHOR | DAMIAN GLYNN BA (HONS) FCA FCILA FUEDI ELAE FIFAA –
DIRECTOR, HEAD OF FINANCIAL RISKS, SEDGWICK INTERNATIONAL UK

3.2 What about loss of attraction?

Loss of attraction is a significantly misunderstood cover.

Currently, there are a lot of positive policy developments, both relating to extensions and newer types of cover (such as cyber). It is difficult to do justice to all of those in one page, and given the pace of evolution in wordings, any commentary offered could be out-of-date before the ink is dry.

Notwithstanding that, at present the majority of covers (and claims) remain predicated on the basis of physical damage, and these considerations assume that this is the cover in force.

This would require damage to something nearby that ordinarily pulls customers to the client.

However, clients may assume that if their business becomes less attractive, any loss arising will be covered.

That is not the case, and the risk of expectations not being met is high. Even among practitioners, there can be discussion about ‘gaps’ in business interruption cover. If the starting presumption is that everything is covered then there will be plenty of ‘gaps’ appearing, and clients will feel permanently short changed.

When advising clients to take out loss of attraction cover, it is important to be clear about what that provides, and what it does not.

Salient points to highlight include:

- This cover requires damage to a property in the vicinity of the client’s business

- Damage in this context is often undefined within the policy wording but insurers are likely to have intended that to mean actual physical damage
- Vicinity is often undefined, but where a definition is included, that is typically within a one mile radius of the insured premises
- The damage (and not anything else) must cause a reduction in the number of customers visiting the client

Examples of what would constitute an attraction include:

- A theatre adjacent to a restaurant, the latter patronised largely by people attending an event at the theatre.
- A stately home that also attracts visitors to a tea room in its vicinity
- A popular retailer serving as an anchor store in an out of town shopping centre

Examples of circumstances where a policy would not respond include:

- General economic downturn
- Disinclination on the part of customers to leave their homes (for example when there is heavy snowfall)
- Downturn due to the general blemishing of the reputation of a place after an incident (such as the Salisbury Novichok attack)
- Unavailability of a natural attraction (such as a mountain or the countryside) causing visitor numbers to fall - for example Foot & Mouth outbreak on land near a hotel.

The fact that policies will not respond to these circumstances is not a gap in cover – it merely reflects the fact that such things are not normally insurable.

To avoid expectation issues, if there is a specific concern about the impact that damage to property in the vicinity could have on a client’s business, it might be wise to explicitly clarify with underwriters at the outset that such property constitutes an attraction.

Loss of attraction cover may be available as an extension to some commercial policies but this may not be available for SME package type policies.

One final note – the discussion above has addressed loss of attraction cover in isolation. There are wordings that hybridise this cover with other extensions, such as denial of access or notifiable disease outbreaks. Those wordings can offer superior cover (a reduced number of extensions might equate to a reduced number of gaps in cover for claims to fall between), but being clear on the scope of that is something that brokers may wish to consider to avoid the perception of any cover ‘gap’.

POINTS TO CONSIDER

- Careful consideration of policy terms including ‘Damage’ and ‘Vicinity’
- LoA Cover may be available as an extension
- Each risk will present its own unique features determining whether loss of attraction may be required

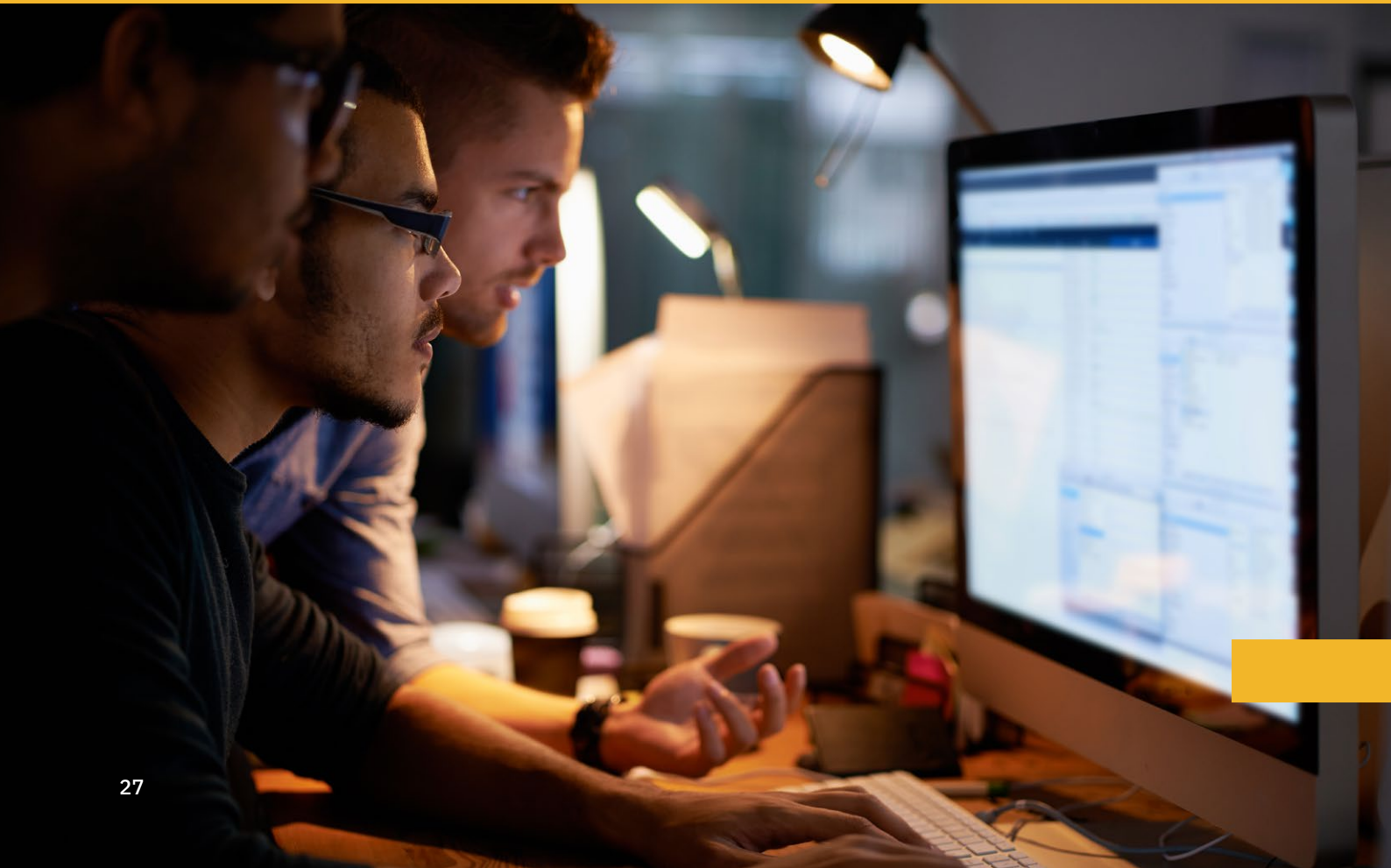
CYBER

AUTHOR | STEVE COATES ACII – CHIEF UNDERWRITING OFFICER, POOL REINSURANCE COMPANY LTD

4.1 Cyber terrorism property damage

Terrorism schemes were essentially created to address the conventional manifestation of terrorists causing damage. This was primarily achieved through using traditional methods such as person or vehicle borne improvised explosive devices, or aircraft. However, the common thread in any of these was that the terrorists had to firstly create or gain access to the means of damage and then find a way of bringing it within sufficient proximity of the property so as to cause damage. Since the IRA campaigns and 9/11 attacks, in most developed countries this is more difficult than ever before as the efforts of counter-terrorism agencies cut off traditional attack vectors.

Clearly this is positive news but unfortunately this is where terrorism is somewhat different from natural perils such as storm. Terrorism is a human peril and so when one attack vector becomes more difficult, others may be created. The connected world presents an opportunity for those who wish to use technology for nefarious means. Whether hacktivist, criminal or terrorist, over the past decade it has become possible to disrupt the activities of a business or steal its data or money by remote digital means and one only has to look at the news to see regular occurrences of such incidents.



Of more concern to property, and indeed marine, aviation or energy insurers is the possibility that a malicious actor could cause physical damage to property through the compromise and manipulation of IT systems.

We have already seen some examples of what form such attacks might take with Stuxnet and an attack on a German steel mill in 2014. These may not have been terrorist attacks but they demonstrate the possible attack methods any type of hacker might use.

While terrorists have demonstrated their technical sophistication through both enabling activity and disruptive attacks, they are not believed to currently have the capability to carry out cyber-attacks that could cause physical damage. Nonetheless, several factors, including the increasing difficulty of successfully employing conventional attack methodologies, mean there is a realistic possibility that terrorists will acquire this capability in the future.

Terrorism schemes were not designed with cyber-terrorism in mind and historically cover would not be provided. Pool Re was the first to research and evaluate the risk of cyber-terrorism and in April 2018, extended their cover to include damage caused by remote digital interference.

This is a standard element of their proposition, so all policyholders benefit from the wider cover.

An incident requires certification as terrorist in nature and must cause physical damage to tangible property. Intangible property such as data is not covered, as this is more specifically addressed by the cyber market, and nor is money. Computer equipment is covered for fire and perils, but not accidental damage.

Pool Re is now working with academic partners, such as the Cambridge Centre for Risk Studies, to further evaluate and quantify the future risk of cyber-terrorism. Additional focus is also being placed on risk mitigation in order to help Pool Re member insurers promote IT security best practice and make it more difficult for malicious actors to gain access to policyholders' IT environments and data. To this end Pool Re published a cyber risk mitigation guide in Q1 2019 promoting some of the tools and techniques that have been created already from both government agencies such as National Cyber Security Centre (NCSC), and the private sector. This guide can be accessed at www.poolre.co.uk

POINTS TO CONSIDER

- There is the possibility that a malicious actor could cause physical damage to property through the compromise and manipulation of IT systems
- Intangible property such as data is not covered, as this is more specifically addressed by the cyber market, and nor is money
- Pool Re published a cyber risk mitigation guide in Q1 2019 www.poolre.co.uk

AUTHOR | JAMES BURNS – CYBER PRODUCT LEADER, CFC UNDERWRITING LTD

4.2 Terrorism cover elements within specialist cyber insurance policies

Technology has fundamentally changed the risks we face day-to-day. Many crimes and malicious attacks that were once committed physically are now carried out online. As a result of this shift, cyber insurance has been developed as a solution through which organisations can protect themselves from the increasingly severe financial fall-out caused by these growing risks.

To date the majority of cyber attacks have been criminals looking for new opportunities. However, their success shows the path terrorists could follow to weaponise cyber. It is possible that some terrorist groups will develop the capability to wreak havoc on businesses, economies and the public at large through digital means. Like cyber criminals, potential cyber terrorists will look for the weakest link. Given limited resources and low expectation that cyber attacks will affect them, SME's can be seen as the weak link in the supply chain, which makes other businesses and operational assets vulnerable.

One of the main purposes of cyber insurance is to protect intangible assets, like data, from non-physical attacks and this encompasses terrorist attacks too. While we must be careful not to exaggerate the threat of cyber terrorism the means are there. Future cyber terrorists may have the capability to encrypt valuable data sets, take out electronic communications and paralyse business-critical systems. This could cause huge disruption and widespread shutdown of operations for organisations across a myriad of industries and it can all be done without any physical damage taking place.

A progressive insurance market has responded with cyber insurance policies providing cover for these types of cyber terrorist events. From the costs incurred in responding to a non-physical attack to the reimbursement of profits lost as a result of interruption to business operations, cyber insurance has been specially designed to support organisations in mitigating these new digital threats.

A good cyber insurance policy will complement traditional terrorism policies, which cover the physical damage and business interruption, by responding to and covering the non-physical – something which is becoming increasingly important.

POINTS TO CONSIDER

- A good cyber insurance policy will complement traditional terrorism policies, which cover the physical damage and business interruption, by responding to and covering the non-physical incidents.
- The main purposes of cyber insurance is to protect intangible assets like data, from non-physical attacks



RESILIENCE

AUTHOR | STEVE COATES ACII – CHIEF UNDERWRITING OFFICER, POOL REINSURANCE COMPANY LTD

5.1 Pool Re – Vulnerability Self-Assessment Tool

RISK MANAGEMENT AND MITIGATION

There is a mistaken assumption by many that terrorism is a catastrophe peril that cannot be prevented or mitigated. If it happens then it happens and there is nothing to be done about it. This is not wholly correct as while some attacks cannot be prevented others might be especially as terrorists, like thieves, will target risks with poor security. However in many respects this is really no different to storm or flood, where the policyholder can protect their premises as best they can, but if the event is a serious one their premises may be affected anyway.

Terrorist attacks can be prevented or mitigated in the sense that policyholders can make their premises as secure and robust as possible such that the terrorist may decide to target somewhere else with poorer security. There is a small possibility the alternative target may be close enough to the policyholder so as to cause some damage, but this will be less than if the attack took place at the policyholder's premises.

Post-event mitigation is also something to be considered seriously given statistics show that for many of the larger catastrophe events worldwide, there is some correlation between the companies that survive and those who have robust business continuity plans (BCP). This is especially relevant for SMEs who either do not have BCP plans at all, or who have not sufficiently embedded it within their business such that it would be adhered to post-event.

Pool Re has been working with police and government agencies for some time promoting and incentivising tools and techniques such as Crowded Places (a National Counter Terrorism Security Office (NACTSO) initiative for very large venues). In 2018 Pool Re launched a new risk management tool called VSAT (Vulnerability Self-Assessment Tool) which is available for a much larger number of policyholders. This is an on-line self-assessment tool developed by counter-terrorism professionals, and allows a policyholder to self-assess, obtain advice on areas for improvement and receive a discount of 5% from Pool Re premiums if a benchmark standard is attained. The tool is available on the Pool Re website via members and can be used by policyholders with assets insured greater than £50m.

The notion of discounting premiums to reward positive features and/or good behaviours is well established in the insurance industry and it is likely the Pool Re scheme will expand its use of such techniques in the future. Pool Re is also working with its reinsurance, academic and government partners to promote best practice in other areas such as cyber mitigation, as outlined in Chapter 4.

It is also collaborating with Cranfield University and ARL partners (who own VSAT) to train insurance company risk surveyors in counter-terrorism risk management techniques. This will ultimately mean risk management advice for terrorism issues can be provided alongside that given for theft or arson.

POINTS TO CONSIDER

- There is a mistaken assumption by many that terrorism is a catastrophe peril that cannot be prevented or mitigated
- Terrorist attacks can be prevented or mitigated by good security. Possible terrorists may decide to target somewhere else with poorer security
- A Vulnerability Self-Assessment Tool is available for a much larger number of policyholders. These allow a policyholder to self-assess, obtain advice on areas for improvement and receive a discount of 5% from Pool Re premiums

AUTHOR | BIBA

5.2 Businesses Continuity Plans

A business may wish to consider the threat of terrorism and possible impacts to their business when creating a risk register and a Business Continuity Plan (BCP).

As with most other catastrophe perils, a prudent approach to the terrorism threat is to assume the worst and plan for that. Many BCPs assume a terrorism event will not have complicated impacts, but consider the potential of a 'dirty' bomb or a Novichok incident that results in significant contamination and resulting issues around demolition and clean-up before reinstatement may begin. Such an event may result in a long term interruption to a business.

There are many terrorism related issues to be considered in a risk register and BCP, including:

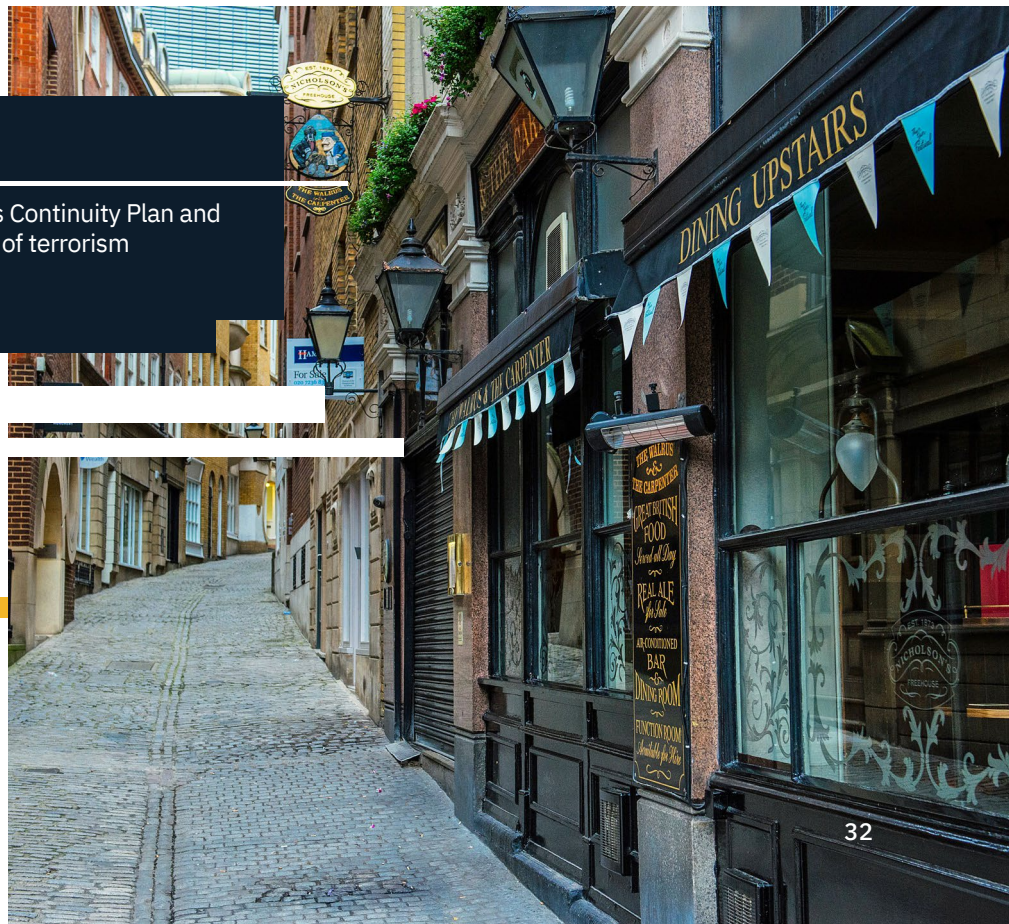
- The decision whether to transfer the terrorism risk to insurance or to self-insure.
- The impact a terrorism event in the vicinity not at your own premises which may deny or hinder access.
- The potential for significant time interruption to a business following a terrorism event
- Supply chain exposures – suppliers plus customers
- Employees – key people and accumulation of employees
- Reputational damage
- Crisis management

A good starting point is the 'Business Continuity for Dummies' book, which is available to order via retailers.

An effective and tested BCP in conjunction with the appropriate terrorism insurance may provide a lifeline for a business in the event of a catastrophic terrorist event.

POINTS TO CONSIDER

- It is good practice to have a Business Continuity Plan and this would often include the impacts of terrorism



AUTHOR | BIBA

5.3 Recognising the terrorism threat

Gov.uk has a helpful section on 'Recognising the terrorist threat'.

Highlights include:

GUIDANCE ON SUSPICIOUS ITEMS

Has it been deliberately concealed, does it have wires or circuit boards, putty or batteries and is it found in a location where people congregate? If so call 999

MAIL HANDLING

It is advisable that procedures cater for all scenarios, is it an unexpected item, bulky or in a jiffy bag and oddly shaped, have excessive sealing, marked 'to be opened by', no return address (or address cannot be verified, unusual postmark, greasy or oily stains emanating from the package or odours emanating from the package? Can the mail handling area be evacuated easily? Also consider having an emergency response plan in place.

BOMB THREAT GUIDANCE

Any member of staff could receive a threat by phone, text, email, and social media or in various other ways. If possible note a caller's number down and do not reply to any messages. Evaluating the credibility of a threat is a critical task, particularly if the threat is imminent. If the threat is believed credible evacuate the building and contact the Police, do not wait for the Police to arrive. Ensure staff are familiar with evacuation procedures.

INSIDER THREAT

There are examples of disaffected staff or an employee that has misrepresented themselves who are willing to take the opportunity to disrupt or cause damage (whether physical or reputational) from the inside. The risks posed by the insider threat can be lessened by carrying out thorough pre-employment checks and by having a strong security culture. The Centre for the Protection of National Infrastructure (CPNI) provides detailed guidance on personnel security www.cpni.gov.uk/personnel-and-people-security

There is much more guidance including – Initial actions after a terrorist major incident, Personal Security training and Guidance for drivers operating commercial vehicles that can be found at www.gov.uk/government/publications/recognising-the-terrorist-threat/recognising-the-terrorist-threat

POINTS TO CONSIDER

- › Check out the full guidance entitled 'Recognising the terrorist threat' on gov.uk and consider staff training as necessary

AUTHOR | ED LEWIS – PARTNER AT LAW FIRM WEIGHTMANS

5.4 Cyber terrorism resilience

Software weaponisation is rapidly advancing cyber terrorism capabilities.

The NotPetya malware is a prime example. What intelligence strongly suggests began as a targeted attack on Ukraine's finance sector spread globally after piggy-backing on transit malware called EternalBlue, released by a group called the ShadowBrokers, paralysing industries from hospitals to marine-cargo. Then there's Triton, a particularly nasty malware that fails the safety systems of petro-chemical plants. Make no mistake, beyond causing disruption these malwares, and many others like them, are intended to create fear and endanger lives.

Combatting cyber terrorism therefore requires enterprise-level resilience, appreciating that people, processes and technology form a complex, interdependent eco-system which needs to be fully reflected in risk profiling and planning.

Hot spots include device controls; network access and application user permissions; as well as merger & acquisition integration. Recognising threats come from within, as well as from outside, is equally vital.

Managing external threats requires dynamic controls to monitor, detect and repair network and application vulnerabilities in real-time. But organisations also need to share experiences with peers and law enforcement, whilst contextualising intelligence to determine not just the severity of potential terror threats but the likelihood of being targeted.

Guarding against threats from within presents arguably the hardest component of the challenge. Malicious insiders often have the advantage of legitimate access and user permissions; however, carelessness can make it just as easy for external threats to penetrate successfully and wreak their effects.

Training on the correct use of IT, security, passwords, 2FA (two-factor authentication), as well as being alert to spoofing and phishing for log-in data, are all vital counter-measures. Thorough vetting of those requiring access to critical controls and assets is also essential.

A particular blind-spot is attitude awareness. Time and again organisations overlook that attitudes drive behaviour, so monitoring network activity to identify prominent rogue elements is not enough. Encouraging employee vigilance to call out those which are more subtle is equally important.

Ultimately effective resilience doesn't happen overnight. It requires fundamental shifts in culture and mindset, achieved by committing to and investing in security, preparedness, staff engagement and education, peer-group collaboration and workplace community.

POINTS TO CONSIDER

- Shore-up resilience against an insider threat
- Audit which staff have access to critical controls and key assets
- Look at the culture and mindset of a business, and the attitudes of its employees, so that rogue elements not only stand out but are much more regularly called out

This update does not attempt to provide a full analysis of those matters with which it deals and is provided for general information purposes only. This update is not intended to constitute legal advice and should not be treated as a substitute for legal advice. Weightmans accepts no responsibility for any loss, which may arise from reliance on the information in this update. The copyright in this update is owned by Weightmans © 2019.

AUTHOR | OFFICIALS FROM THE PROTECTIVE SECURITY SECTION – OFFICE FOR SECURITY AND COUNTER-TERRORISM

5.5 Department for Transport Rental vehicle security scheme

Ultimately, good resilience guards against cyber threats of all kinds, irrespective of their motivation

The Department of Transport has been working closely with several key cross government (Office for Security and Counter Terrorism (OSCT), National Counter Terrorism Police headquarters (NCTPHQ), Law enforcement agencies) and industry stakeholders (inc British Vehicle Rental Leasing Association, United Rental System, Enterprise) partners to develop the Rental Vehicle Security Scheme (RVSS) to help combat terrorism.

The RVSS consists of a 10-point Code of Practice and supporting guide. The code places a commitment on those signing up to (among other things) to:

- › Ensure when handing over vehicles to customers to undertake licence verification checks
- › Lawfully share data and information with law enforcement agencies
- › Appoint a recognised security contact
- › Train staff to identify and report suspicious behaviours
- › Only accept electronic payment for all or part of the rental transaction

The Scheme, which is voluntary, was formally launched on 6 December 2018 and is designed to support the development of a security culture in the vehicle hire industry and is designed to provide deterrence and potential detection of those seeking to use rental vehicles in attacks.

The scheme is available on the gov.uk website and those wishing to join need to complete an application form and declaration that they will produce a security plan outlining how they will meet the requirements of the Code of Practice.

These plans can be the subject of assurance checks by the Department for Transport.

POINTS TO CONSIDER

- › The Rental System Vehicle Security Scheme (RVSS) includes a helpful 10 point code that improves security around the rental vehicle sector



AUTHOR | THE CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE (CPNI)

5.6 Security Considerations Assessment (SCA)

In April 2019, the Centre for the Protection of National Infrastructure (CPNI) launched guidance for businesses and services to assess their consideration of, and response to, security-related vulnerabilities across a range of activities and processes.

SCA also helps to ensure that where security risks exceed an organisation's risk appetite, physical, personnel, cyber and cross-cutting security measures are properly embedded in a multi-layered approach.

If correctly implemented this may be an important tool to protect people, buildings, infrastructure, information, and the systems that support organisations from those with hostile and malicious intent, whether they use physical and/or cyber-attack methods.

The SCA document is intended for use by those who are accountable and responsible for the creation, planning, design, construction, manufacture, use, operation, management, modification, improvement, demolition and/or recycling of individual assets or products, or the wider built environment, as well as those involved in the provision of related services. It is also for the use of those organisations who wish to protect their commercial information, personal data and intellectual property.

You can find more information here:
www.cpni.gov.uk/security-considerations-assessment

POINTS TO CONSIDER

- ▶ Check out the Security Considerations Assessment (SCA) to ensure that potential security-related vulnerabilities are considered.



CLAIMS

AUTHOR | STEVE COATES ACII – CHIEF UNDERWRITING OFFICER, POOL REINSURANCE COMPANY LTD

6.1 Pool Re claims process

CLAIMS

Pool Re insurer members deal with terrorism claims for their policyholders like any other category of claim, maintaining normal claims procedures and service standards regardless of whether any ultimate reinsurance claim is made against the Pool Re scheme.

Pool Re requires that insurers take care to identify the cover provided; in terms of the general policy cover as well as the attachment of terrorism reinsurance cover. Pool Re also has direct control over high value claims and may undertake an audit on any claims. There is a three-point oversight and validation process.

Three Point Oversight Process

1. Policyholder claims over £10,000 must be assigned to qualified loss adjusters;
2. Policyholder claims over the Pool Re member's large loss thresholds are referred to Pool Re for sign-off;
3. Reinsurance claims over £10m are referred to HM Treasury for sign-off.

Technical validation process for large losses, covering:

1. Policy coverage;
2. Technical; and
3. Financial accuracy.



NOTIFICATION AND CERTIFICATION OF A TERRORISM EVENT

An act of terrorism is defined as 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.

- Insurer members notify Pool Re of any potential terrorism events;
- Pool Re requests formal certification of the event from HM Treasury;
- HM Treasury has 21 days to certify;
- Failure to certify leads to an independent tribunal process for a final and binding decision;
- Certification allows Pool Re member companies to claim against their reinsurance agreement.

POLICY COVERAGE

Certification ensures that the general cover provided to policyholders is replaced by the extended reinsurance cover offered under the Pool Re Scheme. Pool Re members use the same definitions of terrorism within their general terrorism exclusions as used by Pool Re. This means cover is back-to-back and this concept is explained more fully in Chapter 2.

Cover also includes loss or damage arising on an 'All-Risks' basis which includes certain non-conventional covers; CBRN (Chemical Biological Radiation and Nuclear) and remote digital interference.

The scope of cover for CBRN is wide and has little previous legal or insurance market precedence as to the understanding of the application of such cover. Issues may arise with the disposal of contaminants and contaminated materials, the availability of expertise to attend the clean-up, and knowledge of at what point decontamination is successful and the insurer's obligations fulfilled.

Pool Re has robust processes in place to ensure the effective handling of catastrophic or surge type events. This also includes assisting its insurer members, loss adjusters and other insurance industry associations, in understanding the specific complexities that may arise from a large-scale terrorism event.

MANAGING POOL RE MEMBER'S RETENTIONS AND REINSURANCE CLAIMS

While Pool Re members handle their individual policyholder claims, they are required to report all claims to Pool Re through quarterly bordereaux of policyholder claims. These serve as the basis of any reinsurance claim against the Pool Re Scheme.

Pool Re members also provide specific details of individual policyholder large losses for consideration by Pool Re. Pool Re agrees and monitors the progress of these claims prior to their inclusion in any reinsurance claim submissions for reimbursement. Large losses are defined as individual original insured claims exceeding 50% of the member's per event retention, or £1m, whichever is the lesser.

POINTS TO CONSIDER

- Terrorism events must be certified by HM Treasury or an independent tribunal in the event of a dispute. Certification allows Pool Re member companies to claim against their reinsurance agreement
- Certification ensures that the general cover provided to policyholders is replaced by the extended reinsurance cover offered under the Pool Re Scheme
- The member insurer handles the claim as they would any other property claim, but if Pool Re terrorism has been purchased then they can recover from the scheme

OTHER POLICIES

AUTHOR | LYNNE GROVER-THOMSON – CLAIMS INTEGRITY MANAGER, MOTOR INSURERS' BUREAU

7.1 Motor insurance

Following the terrorist attacks in 2017, when motor vehicles were being used as a weapon, UK motor insurers voted to mutualise the risks associated with terrorism claims. Up until this point, notwithstanding the Road Traffic Act stating that a motor insurer had no liability for incidents of this nature, the Motor Insurers' Bureau's (MIB) Articles of Association meant that the insurer concerned had to pay the claim as Article 75 insurer utilising the terms and conditions of the Uninsured Drivers Agreement. More than 75% of motor insurers (by voting rights) agreed with the change. As a result, Article 75, the relevant element within MIB's Articles of Association, changed to bring these within the scope of the claims paid by MIB.

MIB will now deal with all third-party motor claims for victims of vehicle-related terrorist events on or after 1 January 2019. In the event of a vehicle-related terrorism incident, MIB will look to take the lead and has put in place an emergency response plan to identify the incident and number of victims, initiate a helpline for victims to call and enter into communication with the vehicle insurer.

MIB has purchased a reinsurance programme, led by Munich Re, of £400 million in excess of £100m on an aggregate basis. The first £100m will be retained within MIB.

The definition of terrorism, within Article 75 is as per the Terrorism Act 2000. This is likely to be refined to move closer to the definition used by Pool Re and linked to a determination by HM Treasury where possible.

MIB will take steps immediately to handle claims, if an incident is being treated as if it is a terrorist event. MIB will also liaise closely with the insurer of the vehicle used. In the event of it not being a terrorist event the MIB would pass the claims over to the motor insurer of the vehicle. In taking responsibility for vehicle-related terrorist claims MIB has explored the interaction with HM Government, Pool Re and the Criminal Injuries Compensation Authority depending on the circumstance of the event.

POINTS TO CONSIDER

- ▶ From 1 January 2019 claims arising from a motor vehicle being used as a weapon of terror will be met by the MIB



AUTHOR | JUSTIN GODMAN ACII – CHARTERED INSURER, UNDERWRITING MANAGER - CASUALTY, CNA HARDY

7.2 Casualty/liability

Most UK employers' liability and public liability policies will include inner limits for terrorism. However, aside from these limits, the extent to which terrorism events are covered under liability policies can be silent, in that terrorism cover is neither explicitly included ("affirmative terrorism") or excluded.

Liability policies indemnify policyholders in respect of their legal liability to pay damages and costs. In the absence of a terrorism exclusion, it should follow that the policy will respond to protect the policyholder following a terrorism event, to the extent that the policyholder is found to be legally liable to pay compensation to their employees and/or third parties. The circumstances as to when a policyholder could be found legally liable are somewhat uncertain as there have been no real legal precedents in this area to date.

Liability would most likely arise out of a breach in the policyholder's duty to protect the safety of employees or third parties. Such a breach could result in terrorists accessing a location or it could increase the number or extent of injuries or the scale of damage. Examples of such breaches could include inadequate security arrangements, inadequate screening of employees or inadequate evacuation procedures.

Inner limits for terrorism are usually required for insurers to mitigate the potential aggregated losses from multiple policyholders following a single terrorism event. The vast majority of UK employers' liability policies contain an inner limit in respect of terrorism of £5m. Insurers are unable to exclude terrorism completely from employers' liability policies as a minimum of £5m is required to comply with UK EL legislation.

There is a less consistent approach from insurers on public liability policies, with some insurers providing full policy limits and others applying an inner limit (typically £2m or £5m). Some PL policies will contain an outright exclusion in respect of terrorism, particularly where risks are deemed to represent high terrorism exposures. Other non-standard public liability policies often apply a full exclusion in respect of terrorism.

While some traditional liability policies may not contain explicit terrorism exclusions, some elements of cover may be excluded or restricted by other exclusions contained within the policy, such as war exclusions or cyber exclusions. Within the specialist terrorism insurance market, while primarily aimed at first party property damage and business interruption exposures, cover is available for employers' liability and public liability on an affirmative basis.

POINTS TO CONSIDER

- Liability for terrorism would most likely arise out of a breach in the policyholder's duty to protect the safety of employees or third parties
- Most liability policies will include inner limits for terrorism, with insurers needing to mitigate the potential aggregated losses from multiple policyholders following a single terrorism event

AUTHOR | BIBA

7.3 Home insurance

The way in which terrorism cover is treated in home policies is different to the commercial market.

A number of household wordings include a blanket terrorism exclusion: *Loss, damage, cost or expense of whatever nature directly or indirectly caused by, resulting from or in connection with any act of terrorism.* Followed by a definition of terrorism as: *the use, or threat of use, of biological, chemical and/or nuclear force or contamination by any person(s) whether acting alone or on behalf of or in connection with any organisation(s) or government(s), committed for political, religious, ideological, ethnic or similar purposes or reasons including the intention to influence any government and/ or to put the public or any section of the public in fear.*

Using these standard exclusions and definitions, if a home was damaged as a result of a terrorist driving a vehicle into the property, policy cover would operate under the 'Impact by Vehicle' peril in the policy. However, if the home was damaged by explosion from a bomb planted in a vehicle then cover under a home policy may not operate if the bomb contained biological, chemical or nuclear materials.

For householders and their insurers there is no Pool Re equivalent to protect them from a CBNR terrorist event.

Consider also a theoretical chemical event similar to the Novichok incident at Salisbury but one that is then certified to be a terrorist attack. In this sort of situation, streets could be cordoned off for weeks while the contamination is cleared up.

Businesses with Pool Re terrorism non-damage BI cover would be able to claim whereas home owners would have no recourse to claim for alternative accommodation and would need to pick up the costs themselves.

On the contrary, leasehold flats may be insured for terrorism including CBNR by the freeholder in the commercial insurance market. Here the insuring covenant in the lease will set out what perils are insured and careful consideration is needed by leaseholders around the requirements of their mortgage lender.

The need for blocks of flats to include terrorism cover was clarified in the Upper Tribunal (Lands Chamber) case of *Qdime Ltd v Bath Building (Swindon) Management Co. Ltd & Ors (2014)*. The lease required that the landlord must insure against the explosion peril and the outcome of the case was that terrorism ought to be insured.

Home insurance policy wordings from many leading insurers to Northern Ireland customers include a similar terrorism restriction/exclusion to the home policies offered by those insurers in Great Britain.

POINTS TO CONSIDER

- Terrorism cover for home insurance policies differs greatly from commercial and may be very limited
- There is no Pool Re for householders
- Cover is available for leaseholders from a quirk which means they may be insured in the commercial market by a freeholder
- Understand the terrorism insurance cover provided by home and commercial insurers
- Consider the demands and needs of customers in relation to terrorism
- In respect of flats insurance, consider the insuring clause in the lease

AUTHOR | DIPESH PATEL – DEPUTY CLASS UNDERWRITER, ACCIDENT AND HEALTH
AND RYAN HUSBANDS – UNDERWRITER ACCIDENT AND HEALTH, DTW1991 LLOYD'S SYNDICATE

7.4 Travel insurance

When reviewing, advising and sourcing travel insurance for clients there are a few things to consider when it comes to terrorism cover. In particular there may be different extensions and levels of cover. It is important to check that terrorism is included.

MEDICAL AND REPATRIATION

The majority of policies will cover terrorism and terrorist events under the Medical Expenses and Repatriation section. However these policies will not normally respond to Nuclear, Chemical or Biological attacks.

CANCELLATION AND CURTAILMENT

Not all policies will offer cover under Cancellation/ Curtailment in respect of terrorist acts and or terrorism at the journey destination.

Policies that do specifically include terrorism will most likely define the radius from the incident and the period of time following the incident where cover will apply.

For example, cover might be restricted to incidents occurring during the holiday or up to 31 days prior to the scheduled departure date of the holiday and to a destination within a 40-mile radius of the incident.

Even where cover is provided under these sections it will only apply where the policy has been purchased and the trip has been booked prior to the occurrence of the incident.

OTHER COVERS

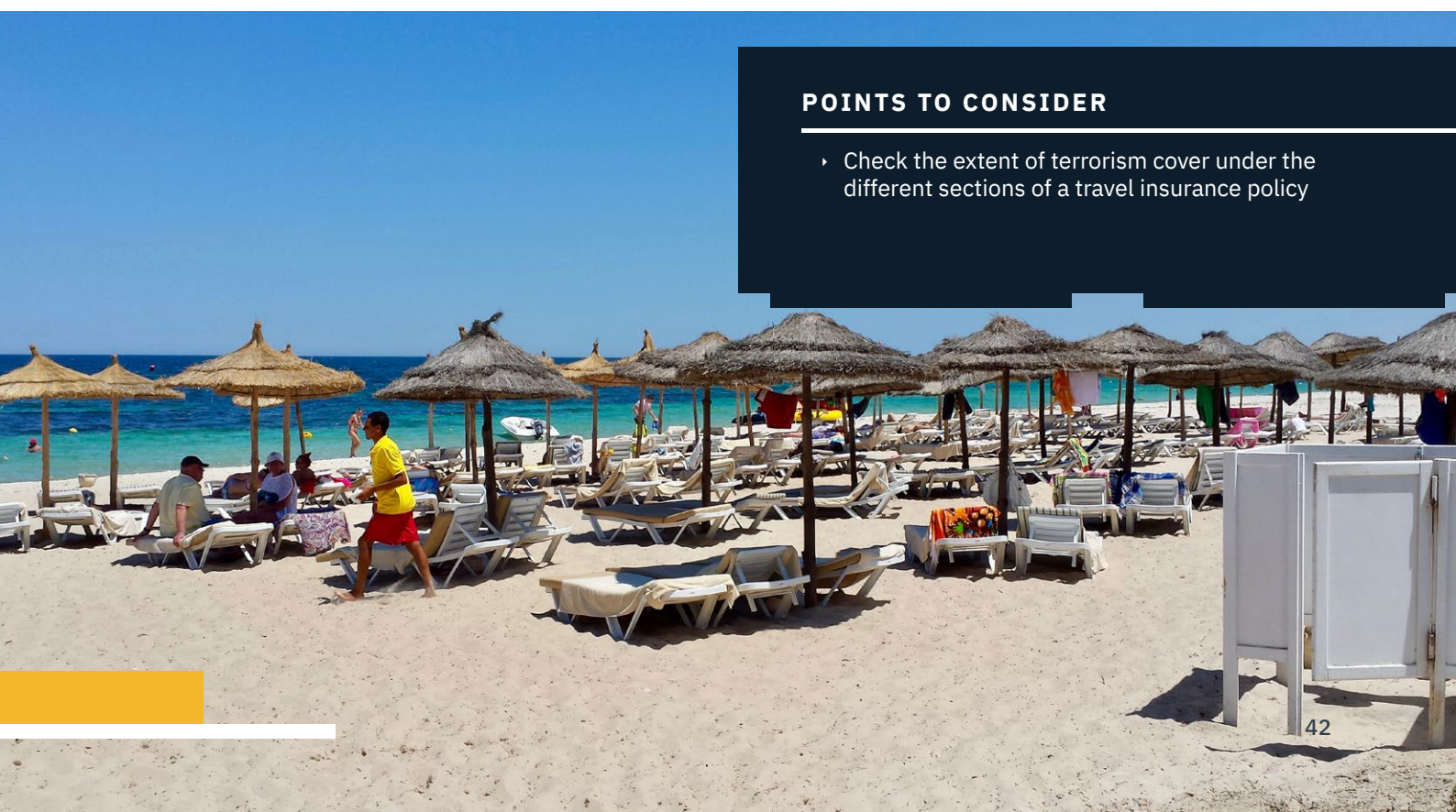
Some policies will cover losses in respect of terrorism and terrorist events under the Personal Accident, Travel Disruption, Baggage, Passport and Money sections of the policy.

This cover is included within the accredited BIBA Holiday Travel+ from DTW1991 scheme.

Visit www.biba.org.uk/schemesandfacilities for more information.

POINTS TO CONSIDER

- › Check the extent of terrorism cover under the different sections of a travel insurance policy



AUTHOR | JONATHAN ROUSE – PARTNER, PROTECT UNDERWRITING LLP

7.5 Different classes of insurance

As the terrorism threat evolves, organisations continue to seek appropriate cover to protect their people, assets and revenues. Traditional terrorism cover remains an excellent way of covering catastrophic physical damage and business interruption, but a range of products have been available for some time, which aim to provide wider protection, against the kinds of events we have seen more recently in the UK.

While the risk of a large vehicle bomb remains a “worst case” scenario, clients are seeking more comprehensive protection against the range of “most likely” attack types. Newer products have widened the event triggers and expanded the indemnification. Importantly, these newer products will respond to events such as London Bridge or Salisbury, which have not been covered by more traditional forms of cover.

By way of example, Attack Insurance is an innovative solution from Protect Underwriting LLP that provides cover whether an attack occurs at or near an insured location, and whether the event is conducted by a terrorist, a criminal gang, a disturbed person or a violent employee. It provides a wide range of responses to safeguard people, protect revenues, build resilience and aid in recovery.

The product has been designed to allow UK medium sized organisations to access the same kind of cover and specialist expertise as multinational corporations, but in a simple and easy-to-purchase package. Attack Insurance has an “aggressor agnostic” set of triggers and provides much broader protection than terrorism. The insured benefits include contents, business interruption, continuing loss, loss of attraction, additional security measures, support from both crisis management and public relations consultants, and assistance with medical expenses including counselling. These innovative products are particularly attractive to organisations in the retail, hospitality or entertainment sectors and where footfall plays a significant role in revenue generation. They are also very attractive to organisations operating in the central business districts of all major UK cities and towns, or those in close proximity to major transport hubs, crowded places or government sites.

POINTS TO CONSIDER

- Policies are available with a wider definition of terrorism and which include acts of war and hostilities which may include incidents such as in Salisbury in 2018



COUNTER
TERRORISM
RESPONSE LEVEL

EIGHTENED

CUSTOMER CHECKLIST

8.1 Customer Checklist - key points to consider

Here are some key considerations which are covered more extensively in the relevant chapters of the guide. These may serve as a useful aide-memoire when thinking about the risk of terrorism and the insurance cover available.

1.1 Why is Terrorism insurance so important?

- › It is important because of the changing threat of terrorism and its unpredictability
- › UK insurance policies vary greatly in relation to terrorism exclusions and the application of sub-limits

1.2 Counter-Terrorism & Border Security Act

- › Ask if insurers have entered into the new agreement allowing them to cede NDBI cover to Pool Re
- › NDBI cover can be added mid-term

1.3 Threat level and response

- › Look at the various government websites, cited throughout this guide, for security information
- › Be aware of changes in threat levels as published by Government

1.4 Incidents are not confined to major cities

- › Terrorism cover is a consideration wherever a business is situated not just in major cities

1.5 Take up of terrorism cover

- › SMEs are as vulnerable as other businesses to financial loss as a result of terrorism
- › There are a number of options available to businesses to obtain terrorism insurance

1.6 Common objections to buying cover

- › Price - cover and price varies to suit most budgets
- › Not appreciating the threat or assuming “it won’t happen to me” – the fact is it might, so terrorism insurance provides certainty
- › Time it takes to get a quote – brokers can simplify the quotation process for clients

2.1 Pool Re

- › Membership of Pool Re is open to any UK authorised insurer
- › Insurers must cede all eligible terrorism insurance risks to the scheme
- › Pool Re cover applies in Great Britain only, not Northern Ireland
- › Pool Re cover includes both material damage and business interruption including NDBI and must be a mirror of a business’ commercial policy
- › War risks are excluded

2.2 Other insurance providers

- › Loss of attraction cover might be valuable for some businesses and not for others
- › Alternative providers can cover risks outside of GB

2.3 Pool Re non-selection rule

- › Pool Re and its members must accept all eligible terrorism risks
- › Policyholders must ensure that all of their insurance risks are insured through Pool Re irrespective of whether they are insured through one or more Pool Re insurers
- › If a business wants to cover only some of its locations, insurers other than Pool Re are available

2.4 Covers

- › Insurers must cede all of a client’s policy exposure to Pool Re
- › Some non-standard risk types eg contingency can be covered by Pool Re if written as a property class

2.5 Chemical, Biological, Radiological, Nuclear

- › The time needed to clean contamination and for debris removal need to be accounted for when deciding on business interruption indemnity periods
- › CBRN terrorism cover is only available from the Pool Re offering

2.6 Northern Ireland

- › In the same way that there are alternative offerings available in the market to Pool Re, there are also insurance solutions for businesses in Northern Ireland for the shortfall in compensation payable under the Criminal Damage (Compensation) (Northern Ireland) Order 1977

3.1 Business Interruption - extensions to cover

- › A business’ cover must sit back to back with the cover provided by Pool Re so that the terms and conditions are reflected in both policies. For example if a primary policy has a suppliers or customers extension or a public utility extension Pool Re also will cover these extensions.
- › Threat or hoax incidents can be covered in the open market

3.2 What about loss of attraction?

- › When looking at loss of attraction cover consider the policy terms including the definitions of damage and vicinity
- › LoA cover may be available as an extension
- › Each risk will have its own unique features determining whether loss of attraction cover may be required

4.1 Cyber terrorism property damage

- › There is a possibility that a criminal could cause physical damage to property through the compromise and manipulation of IT systems.
- › Intangible property such as data is not covered, as this is more specifically addressed by the cyber market, and nor is money.
- › Pool Re published a cyber risk mitigation guide in Q1 2019 www.poolre.co.uk

4.2 Terrorism cover elements within specialist cyber insurance policies

- › A good cyber insurance policy will complement traditional terrorism policies, which cover the physical damage and business interruption, by responding to and covering the non-physical incidents.
- › The main purposes of cyber insurance is to protect intangible assets like data, from non-physical attacks

5.1 Pool Re - Vulnerability Self-Assessment Tool

- › It is not correct to assume that claims caused by terrorism cannot be prevented or mitigated
- › Terrorist attacks can be prevented or mitigated by good security as potential terrorists may choose to target somewhere with poorer security.
- › A Vulnerability Self-Assessment Tools is available which allows a policyholder to self-assess, obtain advice on areas for improvement and receive a discount of 5% from Pool Re premiums

5.2 Businesses Continuity Plans

- › It is good practice to have a Business Continuity Plan and this often includes the impacts of terrorism

5.3 Recognising the terrorism threat

- › Check out the full guidance entitled ‘Recognising the terrorist threat’ on Gov.uk and consider staff training as necessary

5.4 Cyber terrorism resilience

- › Shore up resilience against an insider threat
- › Audit which staff have access to critical controls and key assets

5.5 Department for Transport Rental vehicle security scheme

- › The Rental System Vehicle Security Scheme (RVSS) includes a helpful 10 point code that improves security around the rental vehicle sector

5.6 Security Considerations Assessment

- › Check out the Security Considerations Assessment (SCA) to ensure that potential security-related vulnerabilities are considered

6.1 Pool Re claims process

- › Terrorism events must be certified by HM Treasury or an independent tribunal in the event of a dispute. Certification allows Pool Re member companies to claim against their reinsurance agreement.
- › Certification ensures that the general cover provided to policyholders is replaced by the extended reinsurance cover offered under the Pool Re scheme.
- › Claims must be served within 10 days from the day on which the act giving rise to the claim was committed
- › Claims less than £200 will not be considered
- › Claims may be time barred after six months
- › Compensation may be payable for property damage and consequential loss
- › Property compensation is only payable on an indemnity basis

7.1 Motor Insurance

- › From 1 January 2019 claims arising from a motor vehicle being used as a weapon of terror will be met by the MIB

7.2 Casualty/liability covers

- › Liability for terrorism would most likely arise out of a breach in the policyholder’s duty to protect the safety of employees or third parties.
- › Most liability policies will include inner limits for terrorism, with insurers needing to mitigate the potential aggregated losses from multiple policyholders following a single terrorism event.

7.3 Home Insurance

- › Terrorism for home insurance policies differs greatly and is unusual and can be very limited.

7.4 Travel Insurance

- › Check the extent of terrorism cover under the different sections of a travel insurance policy

7.5 Different classes of insurance

- › Policies are available with a wider definition of terrorism and which include acts of war and hostilities which may include incidents such as in Salisbury in 2018

GLOSSARY

BCP	Business Continuity Plan
BEIS	The Department for Business Energy and Industrial Strategy
BIBA	British Insurance Brokers' Association
CICA	Criminal Injuries Compensation Authority
CBRN	Chemical Biological Radiological and Nuclear
CPNI	Centre for the Protection of National Infrastructure
DfT	The Department for Transport
Franchise	Another form of claims deductible or excess that differs in once it is reached the entire amount of the agreed loss is paid
GCHQ	The Government Communications Head Quarters works with intelligence services (MI5, MI6) and the armed forces to defend Government systems from cyber threat, and keep the public safe, in real life and online
IED	Improvised explosive device
ISP	Information sharing platform
MD/BI	Material damage / business interruption
MIB	Motor Insurers' Bureau
NaCTSO	The National Counter Terrorism Security Office is a police unit that supports the 'protect and prepare' strands of the government's counter terrorism strategy
NCSC	The National Cyber Security Centre was set up to help protect the UK from cyber attacks, and is part of GCHQ
NCTPHQ	National Counter Terrorism Police headquarters
NDBI	Non-damage business interruption
NIRT	Northern Ireland related terrorism
OSCT	Office for Security and Counter Terrorism
Pool Re	Pool Reinsurance Company Limited provides reinsurance to member insurers for property damage and business interruption by terrorist acts within Great Britain
SCA	Security Considerations Assessment
SCaN	See, Check and Notify is a package of measures from CPNI that organisations can deploy to repel hostile intent
SME	Small to medium sized enterprise (business)
Stuxnet	A malicious computer worm used for attacking industrial systems
VSAT	Vulnerability Assessment Tool provided by Pool Re via member insurers for large organisations (assets over £50,000,000) to self-assess their terrorism vulnerabilities

Thank you to all contributors

Steve Coates ACII

Chief Underwriting Officer, Pool Reinsurance Company Limited

Kevin Hancock ACII

Chartered Insurance Broker, Managing Director,
Yutree Insurance Ltd

Gary Barlow

Terrorism Underwriting Manager, NMU (Specialty) Ltd

Damian Glynn BA (HONS) FCA FCILA FUEDI ELAE FIFAA

Director, Head of Financial Risks, Sedgwick International UK

Ed Lewis

Partner, Weightmans

The Protective Security Section

– Office for Security and Counter-Terrorism

Lynne Grover-Thomson

Claims Integrity Manager, Motor Insurers' Bureau

Justin Godman ACII

Chartered Insurer, Underwriting Manager - Casualty, CNA Hardy

Dipesh Patel

Deputy Class Underwriter, Accident & Health -
DTW1991 Lloyd's Syndicate

Ryan Husbands

Underwriter, Accident & Health, DTW1991 Lloyd's Syndicate

Jonathan Rouse

Partner, Protect Underwriting LLP

**Officials from the Centre for the Protection of
National Infrastructure (CPNI)**

James Burns


Cyber Product Leader, CFC Underwriting Ltd

**Compensation Services - Department of Justice
for Northern Ireland**

The BIBA Property Committee

Designed and produced by

Whistle
www.whistle.agency



☎ 0344 770 0266

✉ enquiries@biba.org.uk

🖱 www.biba.org.uk

🐦 @bibabroker

🌐 BIBA

📍 Find Insurance 0370 950 1790