AIG Terrorism White Paper

Global terrorism: On high alert!

A changing terrorism MO and what it means for your business

AIG®

in association with RUSI and NYA International

Terrorism remains a significant threat to businesses and communities the world over and does not just take one form. ISIS is currently the most active group after entering a new phase of inciting attacks beyond its immediate borders in 2015. AIG, in partnership with the Royal United Services Institute (RUSI) and NYA International, considers what this means for businesses, how the threat could manifest itself and how organisations should prepare.

Part One: From hard to soft targets... how and why terrorists made the shift

ISIS may be losing territory but it retains an ability to inspire individuals and groups outside of its heartlands in Iraq, Syria and Libya. This has been evident in the many ISIS-inspired attacks in various European cities. The threat posed by returning foreign fighters is also increasing.

While it can be argued that civilians have always been targeted in terrorist attacks – with nearly 3,000 people killed on one day in the 9/11 attacks in 2001- the intention to target civilians by groups such as ISIS has never been as explicit or so easily communicated. These terrorist groups increasingly look to inspire acolytes through deft online propaganda videos.

Since the Mumbai marauding attacks of 2008, groups such as ISIS, Lashkar-e-Toiba and Al-Shabaab have increasingly shifted attention to soft targets. The Mumbai attacks demonstrated how several well-armed individuals with small explosive devices and automatic weapons could cause significant loss of life by attacking a heavily-populated area and easily accessible public buildings.

In many ways Mumbai was a major precedent, inspiring subsequent marauding terrorist firearms attacks (MTFA), including those in Nairobi 2013, Tunisia June 2015, Paris November 2015 and Istanbul on New Year's Day 2017. Armed assaults – used in around 20% of all terrorist attacks – are more deadly than other forms of attack. Just over half of attacks on civilians utilise bombings and explosions. In 2015, there were over 12,500 civilian deaths arising from terrorist attacks, an increase of 550% since 2000[i].

The Global Terrorism Index defines terrorism as:

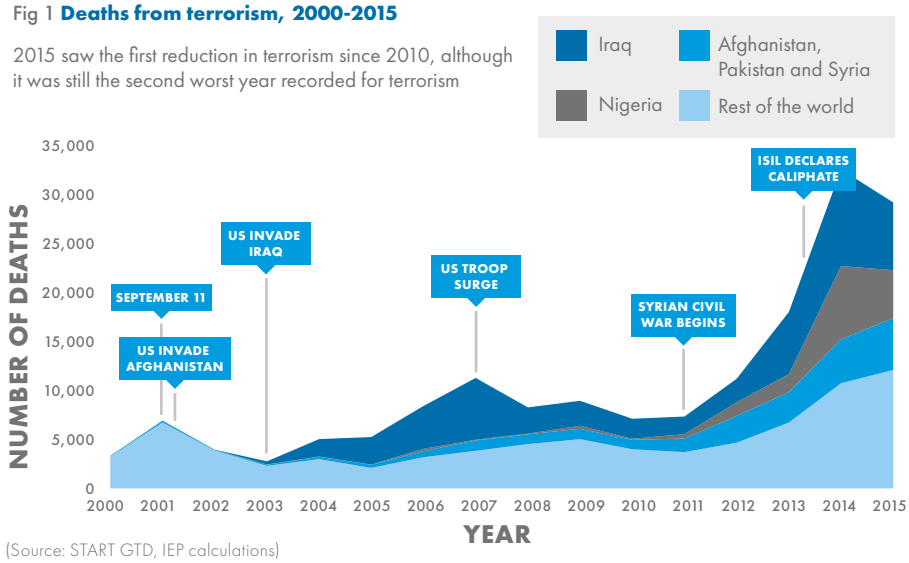
"The threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation".

This definition recognises that terrorism is not only the physical act of an attack, but also the psychological impact it has on a society for many years after.

Terrorist organisations such as ISIS are actively encouraging their followers to target civilians in Western countries

Fig 1 **Deaths from terrorism, 2000-2015**

2015 saw the first reduction in terrorism since 2010, although it was still the second worst year recorded for terrorism



(Source: START GTD, IEP calculations)

Top trends in terrorism
(source: Global Terrorism Index)

- Private citizens and soft targets (e.g. restaurants, shopping malls, museums and hotels) are increasingly targeted
- Improvements in counter-terrorism surveillance have increased the likelihood of more complex plots being intercepted
- Two groups - Boko Haram and ISIS - are responsible for half the deaths from terrorism, with ISIS in particular encouraging attacks in OECD countries

[i] http://www.visionofhumanity.org/sites/default/files/Global%20Terrorism%20Index%202016_0.pdf

Inspiring lone actors

Lone-actor attacks, such as those in Nice in 2016, Sydney in 2014 and Norway in 2011, are the most frequent type of terrorist activity in the Western world. This type of attack is responsible for 70% of all deaths from terrorism in the West since 2006[ii]. In 2015 there were 33 lone actor attacks in connection with ISIS, up from 13 in 2014.

Until the end of July 2016, there were 22 ISIS-inspired lone actor attacks, including the Nice truck attack which killed 85 and the Orlando, Florida, night club shooting, which killed 50. More recent events include the truck attack by Tunisian Anis Imri in a Berlin Christmas market, which killed 12 people in December 2016, and the massacre of 39 people by a lone gunman in a nightclub in Istanbul in the early hours of New Year's Day 2017.

In RUSI's analysis of lone-actor plots in Europe, nearly a third used firearms, 17% involved explosives and 12% involved blades. For nearly a decade, Islamic extremists have encouraged the use of a wide range of attacks. This includes those that are easy to carry out, involving vehicles and knives, such as the Nice and Woolwich attacks (with attackers in the latter buying their main weapon from a home improvement store).

In spite of the increased number of deaths from terrorism in the West, 2015 saw the first drop in overall deaths since 2010, due to the weakening of ISIS and Boko Haram in their core areas.

Growing threat for OECD countries

2015 was a particularly bad year for OECD countries, which experienced a 650% rise (to 577 in 2015 from 77 in 2014) in the number of fatalities resulting from terrorism, according to the Global Terrorism Index 2016 (GTI), published by the Institute for Economics and Peace (IEP). The majority of deaths occurred in Turkey and France and more than half were in connection to ISIS, with attackers in Paris, Brussels and Ankara targeting crowded public places such as sport stadiums, transportation hubs, restaurants and music venues.

The intention to target civilians [in terrorist attacks] has never been as strong, as explicit, or so easily communicated.

These attacks have demonstrated that a very real potential remains for complex operations to be planned and orchestrated. The attacks in France, Belgium and Turkey were amongst the most devastating in the history of these countries and, according to IEP, "reflect a disturbing return of the transnational group-based terrorism more associated with al-Qaeda before and immediately after September 11".

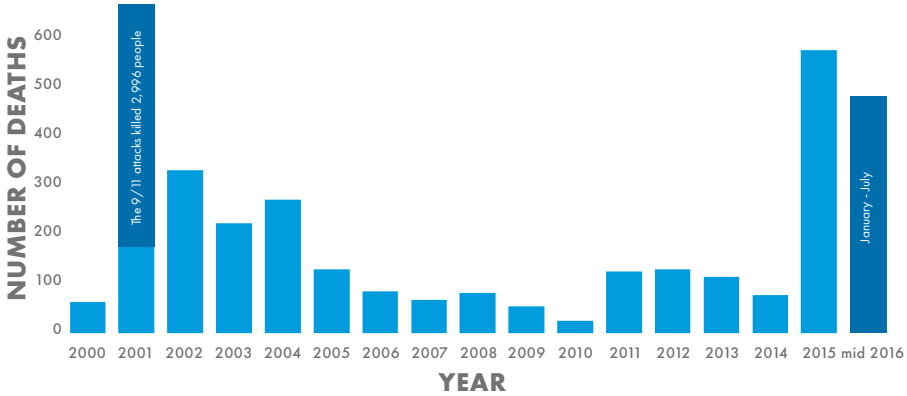
One reason behind the overt targeting of civilians is the goal of creating fear and chaos, and because most public targets are easy to access. Higher per capita spending on counterterrorism vis-à-vis interpersonal violence in countries such as the US and UK "underscores the impact that the fear of terrorism has on the general population," according to the IEP. Meanwhile, empty beaches and resorts in Turkey and Tunisia in the months immediately following attacks there, are also testament to the impact of this strategy.

Counter-terrorism surveillance is another reason for the changing MO of attacks carried out by some terrorist groups. Because there is a high likelihood of complex attacks being intercepted, some terrorist organisations are actively encouraging their followers to plan assaults involving fewer individuals. Therefore, terrorist groups such as ISIS and AQAP seek to inspire smaller-scale attacks while also planning 'spectaculars' like the Paris attacks in November 2015.

An audio message released by the ISIS media arm al-Furqan in May 2016 urged sympathisers in Europe and the US to launch attacks on civilians if they were unable to travel to the group's self-proclaimed caliphate in Syria and Iraq.

Fig 2 **Deaths from terrorism in OECD countries, 2000 to July 2016**

In 2015 deaths from terrorism increased by 650 per cent compared to 2014. This was the second worst year for terrorism in the OECD after 2001 with the September 11 attacks.



(Source: START GTD, IEP calculations, IEP estimates)

[ii] http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf

The internet and social media has made it easier to influence and gain access to the latest generation of susceptible individuals, with ISIS often claiming lone self-radicalised attackers as "soldiers of the Caliphate". "(ISIS) uses the digital world to create an idealised version of itself, a reality show that is designed to find resonance and meaning among its diverse supporters", notes GTI. However, while social media is an important tool, most radicalisation still involves real-world social interaction.

Fears remain that a large, meaningful attack could be waged by ISIS on the West in retribution for the fall of Mosul and impending offensive against Raqqa, which is at the heart of the Caliphate. Current estimates are that between 25,000 and 30,000 fighters, from 100 different countries, have arrived in Syria and Iraq since 2011. Those who have not perished in the conflict could plan attacks on home soil when they return to their countries. Some will have received operational training in explosives assembly and suicide attacks.

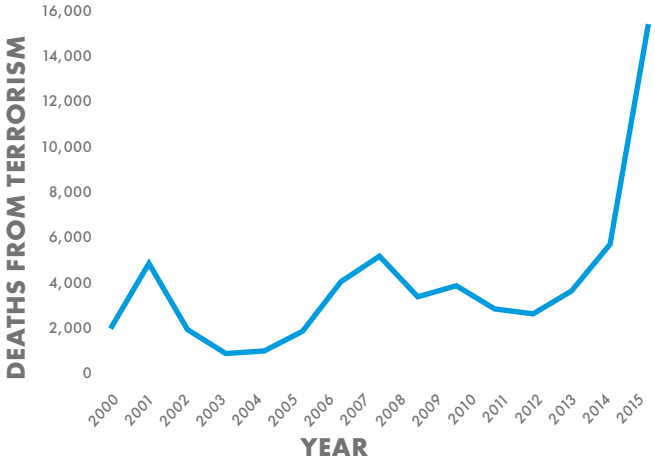
Complex terrorist plots cannot be ruled out, as recent attacks in Paris and Brussels demonstrate.

Some commentators posit that the nature of the current threat environment - with an increased volume of attacks in OECD countries - may be part of an overall strategy to keep these countries under a constant state of heightened security. The intention may be to strain law enforcement resources to deflect attention from more complex plots.

Authorities across Western Europe concede that presently there is a high likelihood of further attacks occurring and that more collaboration is needed through bodies such as Interpol and Europol. In May 2016, FBI director James Comey warned that Europe's lack of coordination on counter-terrorism was leaving it open to attack.

Fig 3 **Deaths from attacks targeting private citizens, 2000-2015**

There has been a 550 per cent increase in the number of deaths of private citizens from terrorism since 2000.



(source: START GTD, IEP calculations)

CASE STUDY

After ISIS

by Andrew Glazzard, director, National Security and Resilience,
Royal United Services Institute (RUSI)

ISIS is staring at defeat and we can look forward to a time when it has largely been eradicated. Or can we?

At the time of writing the Iraqi army was entering Iraq's second city of Mosul, site of Abu Bakr al-Baghdadi's declaration of a new Islamic Caliphate in 2014. Attention is therefore now turning to what happens after ISIS. There is widespread agreement that the fall of ISIS, in Iraq at least, is only a matter of time. Its territorial control has already shrunk significantly from its highpoint in early 2015 and one estimate claims it has lost 25% of territory over that time.

The situation is fundamentally different in Syria, but even there ISIS is under pressure from Turkish forces to the north, opposition fighters to the west, and the Syrian-Russian coalition to the south-west and overhead. ISIS's overseas territories – what it calls walayats (provinces) – are also under pressure, especially in Libya, where it occupies the town of Sirte but not much else, and even that is besieged by US-backed government militias. Its alliances with groups such as Boko Haram in Nigeria do not appear to have amounted to much.

However, in spite of this progress there are good reasons to see the coming period as being one of change and uncertainty rather than renewed safety and security. To understand how ISIS might respond, it is helpful first of all to recognise its multiform nature.

Since its emergence in 2013, experts have argued over whether it is a terrorist group, or guerrilla movement, or a proto-state. In reality, it is all three, and something else besides – a global movement. ISIS will respond to military defeat in different ways according to its different manifestations.

The heartland

ISIS's heartland is its territory in the Tigris and Euphrates valleys, straddling the Iraq-Syria border, with its twin capitals of Mosul and Raqqa in northern Syria. From 2014 to late 2016, anyone living in this region would have experienced ISIS rule, which had nearly all the characteristics of statehood. ISIS ruled through force and intimidation, but also provided services, collected taxes (its main source of revenue), exported raw materials (including to the Syrian regime), hired and fired employees, and administered the law.

Losing this territory will end this experiment in governance. While most observers assumed that it would be more difficult to remove ISIS from northern Syria, where the international coalition's room for manoeuvre was more restricted, at the time of writing the Syrian Democratic Forces, aided by coalition airstrikes, have reached ISIS's main Syrian stronghold of Raqqa. As long as the Euphrates valley remains available to ISIS, it will continue to claim to operate a state, and seek to maintain a fiction that this is the renewed Caliphate.

In vacating northern Iraq, ISIS will inevitably leave a power vacuum. What fills this vacuum will be crucial to Iraq's long-term security and well-being, and there is no doubt that a great deal of political and diplomatic capital is being expended by a wide range of actors inside and outside Iraq to ensure that what comes next meets the country's needs. Everyone – except ISIS – will want stability, but on their own terms.

A lack of cohesion between the Shia majority, the Sunni Arabs who make up the most substantial minority, and the (mostly Sunni) Kurds continues to be Iraq's most fundamental challenge. Each of those groups fear domination by the others, and each operates armed militias, or has sought the protection of external forces, or both. Those external forces, meanwhile, are fighting several proxy wars in Iraq as well as Syria. The outlook is therefore unpredictable, but most scenarios are bleak.

There are good reasons for thinking that Iraq will remain seriously unstable post-ISIS. ISIS' predecessor organisations, al-Qaeda in Iraq (AQI) and Islamic State of Iraq (ISI), thrived from 2003 to 2006/2007, and ISIS came back from apparent defeat in 2010 stronger than ever. Many of the political conditions that enabled AQI/ISI largely remain.

These include disastrously poor governance from Baghdad, sectarian polarisation, a weak army and police force at odds with some very strong militias and paramilitaries. Interference by neighbouring countries, especially Iran, is another factor. Indeed, some of these conditions are worse today, as a result of intervention from overseas and Baghdad's over-reliance on militias, some of which it cannot control.

At the heart of the post-ISIS problem in Iraq will be the perceptions of the Sunni Arabs – largely disenfranchised, fearful of Shia domination, and many with little to lose. In the absence of a political settlement that binds in Iraq's largest minority, an ISIS successor is a real possibility.

The periphery

ISIS's guerrilla activities are evident just outside its heartland. Its attack on Kirkuk in October 2016, just as the Iraqi army was making rapid progress towards Mosul, illustrates its potency as a guerrilla force.

What is more, ISIS has available to it an extremely useful asset to any insurgent force: a border. ISIS and its predecessor organisations have long experience of utilising the Syria-Iraq border to their advantage. It goes back to the early days of the insurgency when al-Assad's government cynically supported Sunni Islamist forces as they harried coalition forces in Iraq from the borderlands.

ISIS will retain its Syrian base for some time to come and use this to attack Iraq. Even when ISIS is removed from Raqqa, whether by coalition or Syrian regime/Russian forces, it will become a destructive insurgent force in many parts of Syria. The war-torn state will simply not be strong enough to police itself internally for many years to come.

The 'Abode of War'

While terrorists do not always need safe havens to be effective, a space in Syria for planning, training and financing terrorism will remain one of ISIS's most treasured assets. Raqqa, its Syrian capital, appears to be its command-centre for terrorist operations in the West and it seems likely that ISIS will seek to increase the tempo of its attacks.

ISIS is not the first group to have compensated for losing territory by increasing its terrorism. But whereas groups such as Al-Shabaab can only operate regionally, ISIS (like al-Qaeda) conceives of all of the West and its allies as the 'Abode of War' – the territories in which attacks can be justified legally.

In addition to its command centre, ISIS has another formidable asset: its intelligence network. In part the legacy of the ex-Baathists in its current and former hierarchy, some of whom worked for Saddam Hussein's intelligence services, ISIS has shown itself to be a master in techniques of infiltration, surveillance, and maintaining covert networks. These networks are believed to radiate out from Syria, through Turkey and into Europe.

With its cadre of foreign terrorist fighters, including thousands from Western Europe, some of whom have returned home or will be making plans to do so, ISIS remains well-placed to continue to strike, and to inspire others to strike. Turkey and Saudi Arabia were singled out for attack in Abu Bakr al-Baghdadi's defiant recorded speech to his supporters as the Iraqi army entered Mosul. The former will probably be most exposed, as ISIS's well-established facilitation networks there can be put to more violent purposes.

North African countries such as Tunisia, which have generated so many of ISIS' foreign fighters, will also be at high threat. And Western European capitals will need to remain on high alert for the foreseeable future, as well as western interests (hotels, embassies, tourist attractions) in many countries around the world.

Global ISIS

Inspiration is what has made ISIS one of the most feared but also influential violent groups in modern history. ISIS's projection of itself as a global movement has drawn recruits from almost every corner of the globe, inspiring lone-actor terrorism in several cities, and alarming governments with the attractiveness of its propaganda. The anthropologist Scott Atran has characterised ISIS as a global, counter-cultural movement, appealing not just to the disaffected and marginalised but to a broader constituency with its self-image of purity, authenticity and power.

The difficulty with combating a movement that draws its strength from being anti-authority is that the more the authorities seek to attack it, whether militarily or through argument or propaganda, the stronger it gets. For this reason, attempts to de-legitimise ISIS may have a polarising effect – they will strengthen the convictions of those who find ISIS abhorrent, while amplifying its appeal for those minded to be sympathetic.

Moreover, some communication on ISIS in the West may actually be counter-productive, as it takes aim at the wrong targets. For instance, the ambition for a Caliphate, according to opinion polls, remains a worthy ideal for a high percentage of the world's Muslims.

It is against ISIS the global brand that events in Iraq may have the greatest, positive effect. Like previous insurgencies from the Mahdist revolt in the Sudan in the 1880s to Hezbollah's wars, a violent challenge to the established order has its greatest appeal when the insurgent is winning. ISIS made much of its astonishing victories against the Iraqi army and its conquest of large parts of Syria in 2014 and 2015.

A space in Syria for planning, training and financing terrorism will remain one of ISIS's most treasured assets

The reality of defeat has already caused a change in tone for ISIS's propagandists, from confident predictions of apocalyptic victory to pleas for patience and predictions of surprising raids against the arrogant Coalition countries. Like other counter-cultural movements before it, the ISIS idea contains the seeds of its own destruction. Perhaps the greatest weapon we can use against it is patience.

The difficulty for the Coalition, though, is that patience will not be enough in the heartland and its periphery. So countering ISIS means doing different things in different places against different manifestations. Above all, it means addressing the governance failures which created ISIS in the first place.

Part Two: From the physical to the virtual. Protecting your people and property

Responding to the threat

Those who protect us from security threats such as terrorism can take a great deal of credit for successfully, and often unobtrusively, reducing our vulnerability to attack, as well as disrupting attacks. According to the National Security Agency (NSA) over 50 potential terrorist attacks on the US have been thwarted due to surveillance.

From sophisticated surveillance algorithms through to highly-engineered security barriers disguised as public benches, the architects and implementers of protective security have undoubtedly made our lives safer. London is said to be the second most watched city in the world, with 420,000 CCTV cameras after Beijing, which has 470,000, according to the latest available figures from Vintech in 2011. Chicago, Houston and New York are said to be the US cities with the highest number of surveillance cameras. Intelligence services are increasingly making use of high-tech tools, including facial recognition and voiceprint, to monitor suspects and intercept communications.

However, even the most intuitive protective security measures can be overcome. Malicious actors are often highly-innovative and spend a great deal of time doing research and development of their own, identifying vulnerabilities and developing new ways of defeating counter-measures. In protective security and counterterrorism, as in many other fields, there is a knowledge curve, and malicious actors strive to be ahead of it.

The domestic threat

While the chance of getting caught up in a terrorist attack remains extremely remote, businesses need to consider the safety of their employees as they go about their day-to-day business. They also need to consider their response if indirectly affected, for instance if transportation systems or city centres are shut down in the aftermath of an event.

It is clear that many business leaders are already alert to the threat. According to research carried out by AIG and Ipsos MORI in the UK in 2016, forty percent of business leaders are fairly or very concerned about the vulnerability of their people in the UK to terrorism. Thirty-seven percent were concerned about terrorism impacting their business premises while a significant 55% were concerned about the impact of terrorist activities impacting computer networks.[iii]

Situational awareness training for corporate security and other personnel can help staff to recognise potential risks and vulnerabilities with the aim of creating a more alert workforce. Everyone in an organisation should be part of the overall security awareness programme, not just security professionals. Among other things, staff need to be able to identify and report suspicious behaviour, e.g. individuals wearing unseasonable clothing (which could conceal weapons) or who appear to be conducting reconnaissance.

Situational awareness training can help create a more alert workforce.

Situational awareness is "being aware of what is occurring in your immediate area and recognising a potential threat at an early enough stage to allow counter measures to be taken to avoid it"[iv]. While a basic building block for law enforcement, military and intelligence professionals, the general public is typically not as attuned to detecting abnormal behaviour or unusual activity. In London, the UK government and British Transport Police launched its "See it. Say it. Sorted" campaign in November 2016 in an effort to encourage commuters to be their "eyes and ears".

[iii] The research involved face to face interviews with 114 C-suite and executive board level respondents from top 500 companies by turnover and top 100 by capital in the UK between September and December 2016.

[iv] GP McGovern: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/mcgovern-situational-awareness-in-terrorism/278

People are an organisation's greatest asset but also its greatest source of potential vulnerability

Locational awareness is also important. Following 9/11 there was a strong focus on the risk surrounding iconic buildings. Many larger firms chose to locate staff in several different offices and avoided major skyscrapers and other landmarks. However, the MO of recent attacks suggests that companies must now consider other situational risk factors, such as proximity to shopping centres, transport hubs, concert venues and tourist attractions.

In the aftermath of the Brussels airport attack, one suggestion was made to move check-in queues to the outside of the building. It is understood this suggestion was quickly shot down by risk consultants, who explained that such a move would simply shift the main target (civilians) to a more vulnerable location.

AIG recently advised a publishing house situated close to one of London's major train stations on how they should react if a marauding attack in the station were to occur and spill over into the surrounding area. Important considerations include how quickly the building could lock lobby doors and close-off lift and stairwell access to floors above.

An organisation and its security personnel need to be prepared to go into lockdown during the critical period just after a major event and before emergency services arrive (known as the "dead zone"). In addition to first-aid training, frontline personnel need to be able to triage - to prioritise, treat and remove casualties in order to save as many lives as possible.

In the case of a marauding attack, the response is to detect, delay, deny (access) and defend. External security guides and CCTV are essential tools in protecting the perimeter, while internal security guards should be considered a second line of defence. Businesses should also be more alert during certain times of day when their employees are in transit and most vulnerable to attack (e.g. morning and afternoon rush hour and during lunch).

In certain sectors, "active shooter" training may be appropriate. With the mantra of "Run, Hide, Fight" staff are taught how to find exits, barricade doors with office furniture and improvise weaponry with realistic drills and rehearsals. Post the 1999 Columbine High School shootings in Colorado, such training has become increasingly common in the US for schools, colleges and businesses.

However, while generally accepted in a country where there is a high level of gun violence and 70% of active shooter attacks take place in a business[v], elsewhere cultural acceptance is significantly lower. HR professionals are keen to strike a balance between adequate workplace safety training and not wanting to scare their employees.

One way to broach such a challenge is to incorporate some elements of active shooter training as part of fire response training exercises and drills. Companies should challenge existing protocols to make sure they are fit for purpose, or adopt new ones. A fire alarm could tell staff to evacuate, but a different alarm might mean the building is under attack and staff need to hide, for instance.

People are an organisation's greatest asset but also its greatest source of potential vulnerability. Governments have depended on security vetting for many years and systems have become increasingly sophisticated. While no system is fool-proof, behavioural research can help security professionals identify and, just as importantly, manage personnel risks. Personnel security is not just vetting but about a wide range of behaviours – such as workplace culture and morale, or individuals' propensity for compliance.

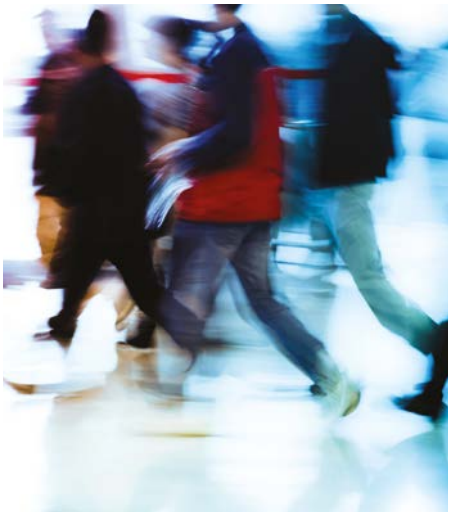
One vulnerability that should be considered is the vulnerable or malicious employee who has access to systems which could cause significant damage in the wrong hands. One way of monitoring individuals with access to key infrastructure is via a buddy system, whereby a colleague checks and approves decisions and actions.

Many experts believe cyber terrorism is the next battleground in the fight against terror, with attackers seeking to inflict physical damage, bodily injury and economic harm by hacking into systems. DDoS attacks that brought down websites in the US, Europe and Liberia in 2016 and WannaCry and Peyta in 2017 have both demonstrated the vulnerability inherent in a hyper-connected world. Former CIA chief Leon Panetta famously warned that the "next Pearl Harbor could be a cyber attack that cripples" America's electrical grid, its security and financial systems.

One of the basic principles of good security is that it should be integrated. In other words, physical, information, cyber and personnel security should be addressed holistically. Ensuring that your building can withstand a vehicle-borne improvised explosive device (IED) is not much use if your personnel policies are so lax that anyone with a smile can gain access to your site. Likewise, investing in the most robust software for intruder detection is money down the drain if you allow staff, contractors, or visitors uncontrolled access to your servers.

[v] FBI

Companies must consider situational risk factors, such as proximity to shopping centres, transport hubs and tourist attractions.



...and the threat overseas

Companies have an increasing duty of care towards their staff given the changing face of global terrorism. Over half of respondents interviewed in the Ipsos MORI AIG research registered concern about the safety of their personnel when travelling overseas, with nearly 40% implementing changes to better protect their staff when abroad.

It is essential to know where employees are, particularly when travelling abroad, and ensuring there are quick and easy methods for them to make contact in the event something goes wrong. Companies may want to consider the following risk mitigation strategies are in place to keep staff safe as they travel on business and work abroad[vi]:

Company travel policy

Clear and simple policies and procedures should enable a company to know where their employees are going, what they are doing and how they can be best prepared and protected during such activities. A company travel policy should ensure the highest possible degree of safety and security for employees when travelling overseas and that all business related travel to risk-rated countries is subject to a formal risk assessment.

Considerations prior to travel

A risk assessment process informs an organisation as to whether more robust training or support is required for business travellers prior to deployment. An up-to-date country travel risk tool can assist with this as it allows a business to risk assess trips in line with its risk appetite and also to monitor situations as they unfold, keeping the business informed in the event that decisions need to be made about its staff in particular locations.

Incident response

It is vital that the company travel policy outlines what employees should do in the event of an incident, for example, who to call and how to behave. Employee responses to incidents need to be in line with the company's corporate crisis management plan which is, in turn, informed to some extent by the insurance policies that are in place.

[vi] Willis Towers Watson: http://www.willis.co.uk/documents/Services/Willis_Risk_Insight_Travel_and_Security_Employers_Duty_of_Care_LR.pdf

CASE STUDY

Expect the best, plan for the worst

by Scott Walker, Manager, Crisis Response, NYA International

During a terrorist attack businesses can really only be reactive: there will be little opportunity to influence the outcome of the incident beyond communicating to staff and customers to either 'lockdown' in a safe location or evacuate, depending on what is deemed the most appropriate way to mitigate loss of life. Due to the chaotic and fast moving nature of such incidents, crisis management teams and other senior security functions will struggle to influence or control events as they unfold.

In this type of situation, the traditional crisis management scenario whereby the decision-making authority and crisis management team make decisions and pass to operational or local teams becomes inverted. The former functions will have much reduced influence, if any at all, in the initial stages of a marauding terrorist firearms incident. Local, often public facing staff such as receptionists, security guards, fire marshalls or floor wardens will be those leading the response.

Statoil's response to the In Amenas gas plant attack, which took place in Algeria in 2013, provides one example. The independent investigation report into the attack – in which five employees died – commended Statoil's contribution to the collective response, specifically concerning the support from leadership to emergency response teams and the clarity and honesty around communications.

Such a response demonstrates duty of care by the organisation if and when the worst happens.

Planning and training

The nature and scale of the recent Paris attacks exposed a lack of sufficient or suitable planning. Many organisations did not know of their staff members' whereabouts and struggled to contact them en masse on a Friday night, with overloaded communications networks and widespread panic.

The incident has led to revitalised interest in crisis communications across Europe, especially mass notification systems, whereby an SMS, recorded message or email is issued to individuals. These can come in the 'push and pull' variety. In the former, a message is sent – i.e. pushed – to a recipient. In the latter, a mechanism such as a pre-recorded voicemail facility is established for individuals to contact. Both push and pull messaging can provide vital communication to employees and stakeholders during an incident and help ensure duty of care.

Companies should plan in advance which departments and individuals own this aspect of the crisis management infrastructure along with who writes and sends the messages. The technology is redundant if employees aren't informed of it, trained in its use or supportive of it.

Established standards – such as ISO 31000:2009 Risk Management and BS 11200:2014 Crisis Management – and physical security management techniques remain relevant despite the evolution of the global terrorist threat. Employed correctly, these approaches offer a means for businesses to order their thoughts, develop appropriate strategies, deploy appropriate resources and prepare effective plans.

Post-incident response

Considering the short timescales and the primacy of state actors in a terrorist incident response, the challenges for businesses are focused as much on post-incident response and recovery, as well as business continuity. It is therefore just as important to plan for the aftermath.

With multiple actors and considerations, post-incident response and recovery is hugely challenging. Businesses caught up in a terrorist incident will typically have to navigate a chaotic scene involving law enforcement agencies, military, government and diplomatic agencies, and international media. Family and employee liaison and – potentially – next-of-kin notification is of primary importance.

Next on the list of chief concerns are crisis communications to all stakeholders, including employees, families, customers, shareholders, the public, the media and law enforcement. Of their own experience, the Statoil report noted, "a systematic approach and resources made available to those involved in [an] incident and their next-of-kin should be embedded in the company's plans for the future."

Part three: Mind the gap: Broadening the scope of terrorism insurance

Terrorism risk is one of the few manmade perils capable of producing a $50 billion-plus loss. For this reason, in many countries, cover for nuclear, biological, chemical and radiological threats is only available via terrorism pools. However, the economic impact on an organisation arising from a terrorist incident may be much greater than the actual physical damage.

In 2015, the global economic impact of terrorism reached $89.6 billion, decreasing by 15% year-on-year, but still the second most costly year for terrorism since 2000. The economic impact of terrorism remains relatively small in comparison to other forms of violence, and is highest in countries where armed conflict is ongoing; however in 2015 and 2016 costs relating to terrorist activities spiked sharply in OECD countries, reflecting an increase in deadly attacks.

There are secondary economic impacts relating to these attacks. In France, for instance, the GDP contribution from tourism fell by $1.7 billion between 2014 and 2015 in the aftermath of the 7 January 2015 Charlie Hebdo shooting and November 2015 Paris attacks. Meanwhile in Italy, which had no deaths from terrorism during that period, the tourism sector grew by $4.9 billion.

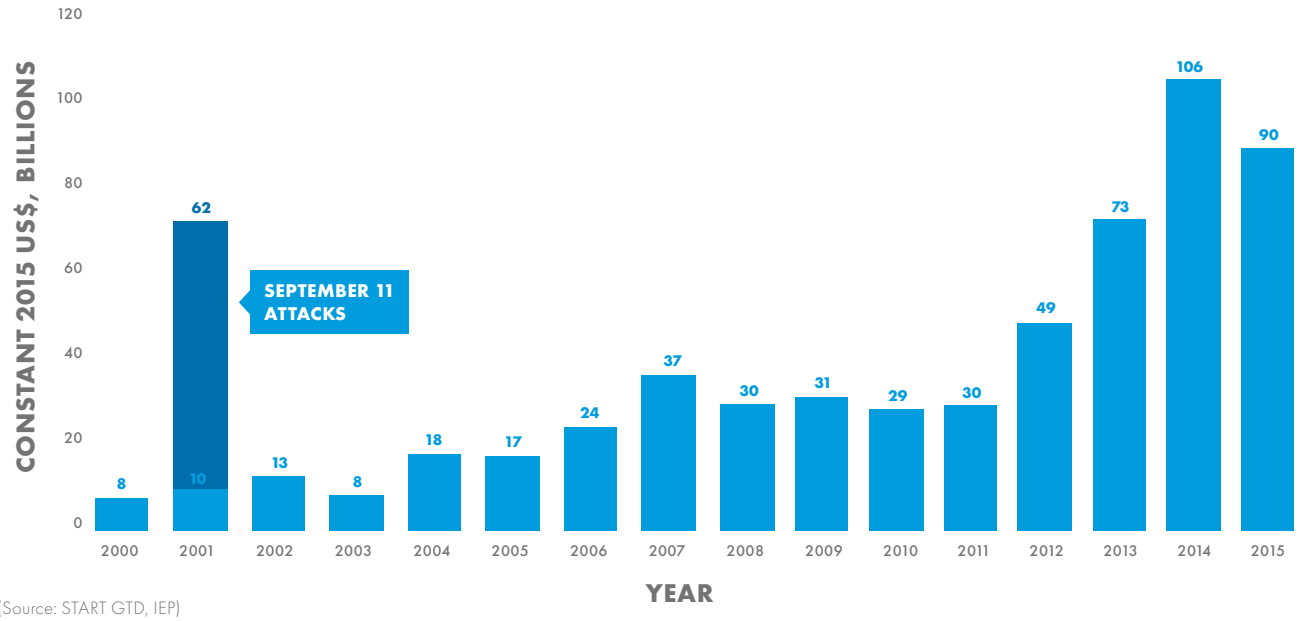
Tourism revenues in Tunisia were down 35% year-on-year after the Sousse attack in which 39 holidaymakers were gunned down as they sunbathed outside the Imperial Marhaba hotel. Tourism's contribution to GDP is twice as large in countries with no terrorist attacks compared to countries with attacks, according to IEP.

Currently, one of the biggest exposures for AIG clients is from a business interruption (BI) standpoint, something that needs to be considered when insurance programmes are put in place. In the aftermath of the Sydney Siege of December 2014 for instance, parts of the CBD - including a pedestrian mall - were shut down by police during what was normally a busy shopping period in the run-up to Christmas.

This type of disruption highlights the need for broad, joined-up coverage, including non-physical damage BI (such as business interruption that is triggered by denial of access). It is however important to note that property policies do not cover the "fear factor", such as the dramatic loss of tourism revenue in countries such as Tunisia and Turkey following attacks and political unrest.

Fig 4 **Economic impact of terrorism, US$ billions, 2000-2015**

Based on IEP's methodology, the global economic costs of terrorism peaked in 2014 and remained high in 2015.



(Source: START GTD, IEP)

In certain regions, terrorist acts are more likely to be financially motivated through activities such as kidnap and ransom and hostage taking. Faced with such exposures, organisations need to ensure they have an extra level of security, training and insurance. Specialist kidnap and ransom insurers and crisis management consultants work with domestic and international authorities to provide clients with the right level of support to manage through often very difficult situations.

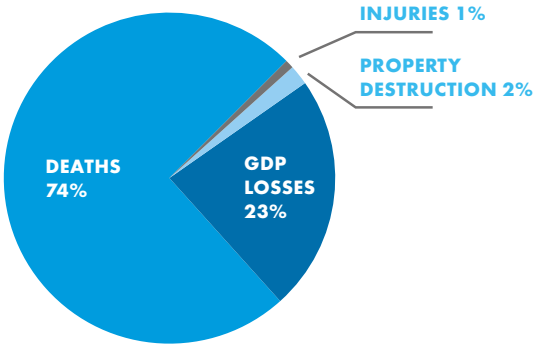
Given the changing nature of the threat, clients are encouraged to look at their overall insurance needs and consider whether terrorism should be purchased as a standalone cover or embedded within a broader property portfolio. One advantage in having both property and terrorism with the same carrier is certainty of cover regardless of the event and its definition.

The Bangkok riots in 2010 and turbulence in the Middle East since 2011 have demonstrated the potential for gaps in cover where terrorism insurance was not in place. The definition of an event (often politically-driven) led to confusion over whether physical damage and/or business interruption arising from an incident should be picked up by property strikes, riots and civil commotion (SRCC) coverage or terrorism, sometimes resulting in claims disputes.

There is currently a movement towards embedded cover, encompassing property, terrorism, business interruption, kidnap for ransom and political violence, which offers clients greater certainty of cover. When discussing specific needs and concerns with insurer and broker partners, insureds should question whether any gaps exist within their insurance programme, as certain extensions may be available to cater to a particular problem (e.g. heavy reliance on one supplier or customer).

Fig 5 **Breakdown of the economic impact of terrorism, 2015**

Fatalities account for 73 per cent of the economic impact of terrorism.



(Source: IEP)

Fig 6 **Economic impact by type of attack, 2015**

CATEGORY	PROPORTION OF ECONOMIC IMPACT
Bombing/explosion	**43.2%**
Armed assault	**18.8%**
Hostage taking	**7.9%**
Assassination	**2.1%**
Facility/infrastructure attack	**0.3%**
Hijacking	**0.1%**
Unarmed assault	**0.1%**
Other/unknown	**27.4%**

(Source: IEP)

Key questions for risk managers and insurance buyers:

What steps are you taking to protect your property and people given the changing nature of the terrorism threat?

Do you understand the secondary impacts an act of terror could have on your business? What contingency plans are in place?

Have you and your insurer partners taken steps to identify and close any gaps in cover?

www.aig.com

AIG®

Bring on tomorrow

GBL00001542 0217