Insurance policy

The first of this year's biannual RISCAuthority Seminars took place last month to explore the key issues facing the insurance industry. **Mark Sennett** was on hand to cover this flagship event

APTLY EMANATING from the Chartered Insurance Institute at 20 Aldermanbury, the RISCAuthority London seminar attracted more than 150 delegates from the insurance sector. The event was chaired by AXA Insurance managing director for underwriting and RISCAuthority chairman David Williams, who kicked off proceedings by announcing the launch of several new key documents and data tools. These include:

- revised version of *Approved Document B: Fire Safety*
- launch of the RISCAuthority INFORMER database – a one-stop-shop for local risk-relevant facts, searchable via postcode
- update to the fire and rescue service response toolkit – an interactive map detailing the most accurate model for fire appliance delivery and local policy
- RISCAuthority large loss statistics
- business sector risk review reports

Government engagement

The first session of the day was delivered by Mark Shepherd, manager of general insurance at the Association of British Insurers (ABI), which boasts more than 250 members and works alongside RISCAuthority to lobby the government for regulatory changes. Mark told delegates that his presentation would highlight two case studies of ABI's engagement with government. The first example of this was its involvement with the shaping of a new Riots Compensation Bill, which has come into fruition following the riots across England in August 2011.

It's estimated that more than £170m of damage was caused during the riots, which lasted for five days. Under current legislation – the Riot (Damages) Act 1886 – the police are liable for damages caused by riots. Following the 2011 riots, the government was keen to explore the possibilities of repealing or reforming the Act due to the high costs incurred, and this was heightened by the recession.

The ABI engaged with the government to highlight the importance of the Act, stating that it provided vital protection for those without insurance or with inadequate cover, and stressing that it was equally vital for the continuation of an effective insurance market. But ABI did concede that the legislation was in need of modernisation, as it was introduced over a century ago!

As a result, an independent review was conducted, with its findings published in November 2013. The recommendations included maintaining the principal of government/state liability, but drastically reducing this to only cover businesses with a turnover of less than £2m per annum. Mark explained that if these recommendations had been implemented before the 2011, the government would only have been liable for 33% of commercial property claims made during the riots and 9% of the total value of commercial property claims. This would have equated to the state being liable for only £1 in every £10 of claims made.

Mark revealed that the amended Bill is expected to be published within days and that it includes a limit of £1m per claim. However, it does not cover business interruption, as the government argued this was not stated in the original Act. Business vehicles damaged in riots will only be covered if they do not have fully comprehensive insurance – meaning the government would only be liable for approximately 4% of business vehicles. The amendments will now go through the parliamentary process for scrutiny before coming into fruition and this will not happen before the general election.

The ABI was engaged with the home office and key government officials since the conclusion of the riots, and had extensive input in both the review and post-review analysis. Mark stressed that this involvement has led to an agreeable solution, which recognises the importance of the Act in safeguarding businesses and maintains an acceptable level of liability for government.

Protecting academies

The second case study focused on the recently introduced Risk Protection Arrangement (RPA) for academy schools. The scheme is described by the government as 'an alternative to insurance', in which losses that arise in academies are covered by UK government funds. The RPA will, as a minimum, cover risks normally included in a standard schools insurance policy. It is a voluntary scheme and academies must opt in. If they do, they will receive a per pupil reduction in their annual grant in return for the cover provided under the RPA. Mark explained the rationale is that it will supposedly provide cost savings and avoid 'complex and time-consuming procurement of commercial insurance cover'.

But insurers are concerned that the scheme represents an implied criticism of the existing market. Other areas of concern include:

- unknown liabilities being funded by government and ultimately the taxpayer, with little/no transparency
- lack of regulatory oversight of the scheme
- uncertainty about financial sustainability of the scheme – potential impact on schools within the scheme
- lack of incentive to manage risk
- government analysis appears to be based on current data and doesn't take account of future trends
- insurers first learned about the intention of the scheme and its implications in May 2014
- no formal consultation with the industry
- no parliamentary scrutiny and no public value for money case has been presented

The initiative went live in September and by the end of January, 918 academies opted into RPA. This represents about £10m in terms of a funding adjustment. Mark said the problem with the current situation is that the existing commercial market is now effectively competing with the RPA. He also fears that this might be the first step towards state-backed insurance schemes being created in other sectors.

Mark concluded that the RPA is an example of how different government departments will work in different ways and there is little central coordination of policy. Even for a well-engaged industry body, ministerial projects can have unexpected and significant impacts. Better outcomes are more likely when we are closely involved and can help shape or influence from as early as stage as possible, but as shown with RPA, the government can choose not to listen.

Building resilience

Brian Watson from metal roofing and cladding systems manufacturer CA Group addressed delegates on the topic of why some buildings are destroyed in a fire and others are not. He started his presentation by questioning why in the UK we don't insist on using non-combustible insulating materials in buildings less than 18m tall. He stressed that if we know a material is combustible, we run a needless risk of it burning when there are safer non-combustible materials on the market.

He then proceeded to give examples of fires that had totally destroyed buildings featuring combustible cladding or insulation. These included:

- an East Midlands retail distribution centre – £50m loss inside 15 minutes of fire
- Sony distribution centre in Enfield – total building loss following April 2011 riots and loss of £75m of stock
- Sainsbury's superstore fire in Chichester in December 2010 – a total loss of the building

A key issued raised by Brian was that fire testing conditions are not exactly replicated during installations on site. He questioned why trims are used in test conditions when they are not used on site. Items such as fillers are often left out for tests, but are used on site; and spans in test conditions are 5m when on site they are normally 8m. Insulation is thicker in test conditions, while in practice 80% of buildings use the back stop. In addition, building regulations have increased insulation thickness, resulting in the fire loads increasing proportionately.

Test conditions also don't take into account insulation being exposed by ridges, hips, verges, corner flashings, windows, doors, and building movement. Another issue is post building penetrations, such as ductwork and ventilation, which can compromise firewalls and compartmentation.

Brian closed his session by saying that it's not logical to use combustible materials in new buildings when there are safer alternatives on the market. He then challenged insurers not to take the risk of insuring buildings that are erected with flammable products.

Waste recycling

Adam Piper from global risk advisory firm Willis explained to delegates that insurance and risk management programmes can be optimised to provide cost-effective protection for waste sites. But he conceded that to get to this stage the main challenge is changing the perception that waste sites pose a significant fire risk. He shared figures from an unnamed

insurance company that in 2012/13 had premium income of £1.5m for underwriting of waste sites but the claims paid totalled £15m!

He pointed out that most fires at these sites happen in external storage areas and in recent years the number of fires has decreased. This he attributed to better management of loss control procedures such as hot work, electrical maintenance/inspection, smoking controls, and exposure management of contractors, security, housekeeping, storage etc.

An increasing presence of physical controls can also reduce the impact of fires, these include:

- roof level sprinklers
- lower level sprinklers
- exposure protection
- electrical room fire suppression
- fire detection
- pre-action sprinklers
- flame detection
- security

Adam highlighted the waste industry's desire to have access to premiums and terms that are 'proportionate to the risk'. To get to this point, he admitted he'd like to see access provided to good quality risk engineering support. Another aim is to have clear standards and guidance, which could be modified and implemented by effective communication with insurers and government. He hopes this collaboration would lead to more fire testing and data benchmarking in order to gain better understanding of the root causes and types of fire.

Cyber crime

The last session of the day was presented by Craig Jones from the Regional Organised Crime Unit (ROCR). He began by telling delegates that cyber crime cost the UK £27bn in 2011 and the cost to the worldwide economy is estimated at more than £1 trillion each year. To fight this, the UK government now allocates £650m per annum to fund the National Cyber Crime Security Programme.

Craig explained that the three main aims of the government in relation to fighting cyber crime are to make the UK the safest place to do business in cyberspace, to make the UK more resilient to cyber attacks, and to help shape an open, stable and vibrant cyberspace that the UK public can use safely and that supports open societies. In order to achieve this, Craig's team has taken a strategic approach, which features the following principles:

- pursue – criminal investigations and activity targeting the top tier cyber threats
- prevent – stopping individuals from becoming involved in cyber crime
- protect – helping businesses and the public aviod becoming victims to cyber crime
- prepare – respond effectively to major attacks and mitigate their impact

The threats posed by cyber crime are continually evolving, are mainly perpetrated remotely and are difficult to trace. The perpetrators come in many different guises including hacktivists, criminals, states and terrorists. The actual means of attack can come from internet fora, malware, distributed denial of service, e-currencies, intrusion, exploit kits and even websites offering cyber crime as a service.

At present if you are a victim of cyber crime in the UK, you can't call 999 to report it. You have to visit the ActionFraud website (***www.actionfraud.police.uk***) and submit the details online, which Craig said is not a satisfactory process, as victims may well be hesitant to share further details online. All complaints are then passed to the National Crime Agency for assessment, and if it feels there's enough evidence to pursue the perpetrator, an investigation will be launched and will often be handed down to ROCR for completion.

Cover confusion

In Craig's opinion, there is still a lot of confusion about cyber crime in the insurance sector. Currently, the few policies on the market do not cover many of the exiting cyber threats, but do generically cover:

- first party damage to data
- business interruption
- privacy and security liability,

including notification and credit monitoring costs
- brand reputation
- cyber extortion
- technology professional liability
- multimedia liability
- Payment Card Industry Data Security Standard (PCI DSS) compliance
- cyber terrorism

Consumers remain unsure if they will be fully protected by insurance and many feel the existing cover on the market isn't worth the cost. Craig stressed that insurers should work with law enforcement, businesses and academic institutions to gain a greater understanding of all the current and evolving cyber threats. He hopes this would lead to the creation of stronger policies that leave no doubt as to what is covered. Despite cyber crime posing a risk to underwriters, it does present a business opportunity for insurers. By offering detailed policies, insurers can help educate businesses about the threats posed by cyber crime and can help educate them to carry out a thorough risk assessment and ultimately leave themselves less exposed.

Craig's closing message was that in order to tackle cyber crime and lessen its economic impact, we first need to work closer together to fully understand the perils. He added that the ethos of prepare, protect, prevent and pursue can not only improve business resilience but act as a deterrent to offenders and commended RISCAuthority's recent cyber risk control publication (*S28: Cyber crime – overview and sources of support*) ■

Mark Sennett is editor of FRM Risk Management, for more information view page 5

The next RISCAuthority Seminar will take place on 4 June at the Radisson Edwardian Manchester. The programme differs from the London event – Damian Glynn from VRS Vericlaim will open the day with a talk on business interruption wording policy and detective superintendent Terry Wilson from New Scotland Yard will present on cyber crime.

For more information on RISCAuthority or if you would like to attend the Manchester Seminar, visit www.riscauthority.co.uk/