AUGUST 2017

CI COMMERCIAL INSURANCE PROFILE

DID YOU KNOW?

If you are an employer, owner, landlord, occupier or anyone else with control of a premises, you are responsible for fire safety. Conducting fire risk assessments helps to prevent fires, keeps the property and employees safe, and increases the chances that your business can recover should a costly fire happen. For more information about how to conduct a fire risk assessment, keep reading.

IN THIS ISSUE

Are You Conducting Thorough Fire Risk Assessments?
The tragic loss of life in the Grenfell Tower fire has far-reaching impacts and highlights the need to undertake formal fire risk assessments of your premises.

Terrorism Underscores Underinsurance Gap
Traditional terrorism insurance no longer provides adequate cover for modern terrorist attacks. Learn what three precautions your organisation can take to financially protect itself from a terrorist attack.

As Risk Gets More Complex, Directors and Officers Are Held More Accountable
Claims against directors and officers have grown more frequent, complex and expensive over the past decade. Learn how your organisation can protect its directors and officers from fines and prosecutions.

Are You Conducting Thorough Fire Risk Assessments?

On 14th June, the London Fire Brigade were called to put out a fire that started in one of Grenfell Tower's 127 flats. The fire then spread to the cladding panels on the building's exterior. Despite the firefighters' best efforts, 79 residents died in the fire. The tragic loss of life has far-reaching impacts and highlights the need to undertake formal fire risk assessments of your premises.

Fire risk assessments are a legal requirement for anyone that owns property or is otherwise in control of commercial premises and other non-domestic premises, such as the common areas of multi-occupied residential buildings. All UK employers with five or more employees are required to keep a written record of their fire risk assessments. While not required for smaller businesses, it is still considered best practice. The government recommends that you review your fire risk assessment annually, as well as after any significant changes to your building.

As an employer or someone responsible for a business or other non-domestic premises, you are responsible for undertaking and reviewing the fire risk assessment. You can do the assessment yourself with the help of industry-specific guides from the Home Office found here. If you do not have the expertise or time to do it yourself, you need to appoint a competent fire risk assessor to undertake the assessment on your behalf. For help choosing a fire risk assessor, follow the London Fire Brigade's eight tips found here. Failing to undertake a fire risk assessment or commissioning an assessor to do it for you could result in fines or imprisonment.

Follow these five basic steps to undertake a fire risk assessment:

1. Identify fire hazards.
2. Identify who is at risk.
3. Evaluate and then remove or reduce the risks.
4. Record your findings, prepare an emergency plan and provide training.
5. Review and update the fire risk assessment annually.

For more information on fire safety and to ensure that you have the most effective cover, contact **Crendon Insurance Brokers Ltd** today.

Crendon Insurance Brokers

Terrorism Underscores Underinsurance Gap

Between 22nd March and 22nd May, there were three terrorist attacks in the United Kingdom, which left 217 injured and 35 dead. These tragic events illustrate how terrorist attacks have changed in recent years. Modern tactics no longer involve coordinated attacks with bombs and sophisticated weapons to cause severe damage. Instead, tactics are more low-tech—often involving heavy vehicles and knives—and focus on injuring or killing as many people as possible. Just as the terrorists' tactics have evolved and changed, so too must insurers' terrorism cover.

Yet, unlike other types of cover, terrorism insurance has remained relatively unchanged. Generally, it only provides an organisation with compensation if its property is damaged in an attack. However, the damage caused by modern terrorism attacks often creates business interruptions rather than property damage. That is why it is important that insurers broaden the scope of terrorism insurance beyond just property damage. However, some terrorism policies may include business interruption as an extension for an additional premium.

In the interim, take the following steps to ensure that your business will not be disrupted by a terrorist attack.

1. **Review your business continuity plan.** If a terrorist attack were to disrupt your day-to-day operations, you need to have a business continuity plan, which outlines how you can continue some—if not all—of your standard business operations.
2. **Develop an emergency response plan.** If a terrorist attack were to happen near your organisation, you need to have a clear plan on how to handle the situation. This should include what actions you and your employees should take.
3. **Discuss and re-evaluate your insurance needs with Crendon Insurance Brokers Ltd.** Talk to your insurance provider about closing any potential gaps in your cover that a terrorist attack could expose.

As Risk Gets More Complex, Directors and Officers Are Held More Accountable

Since the financial crisis in 2008, claims against directors and officers have grown more frequent, complex and expensive. One reason for this rise is government legislation that has increased business transparency and placed the responsibility on directors and officers. In fact, after new guidelines from the Sentencing Council came into force in February 2016, the number of health and safety prosecutions against directors and officers tripled. What's more, the value of the 20 highest fines in 2016 totalled £38.5 million, which was just slightly more than all 660 successful prosecutions in 2015-16.

In addition to stricter legislation, the emergence of new risks—such as cyber breaches—has heightened the circumstances surrounding boardroom decisions. With good cause, as each UK business was hit 230,000 times by cyber attacks in 2016. As a result, 73 per cent of directors and officers are regularly discussing their organisations' cyber security policies, according to a recent industry survey. Unfortunately, despite the increased awareness about the potential cyber dangers, only 57 per cent of all UK organisations have taken action to identify and prevent cyber security risks. Failing to take necessary action on cyber threats could make you and your fellow senior directors liable for fines and prosecutions based on your directors' and officers' responsibility to prioritise cyber defence.

To help ensure that your organisation's directors and officers are complying with government legislation and protecting against cyber threats, consider adopting the following best practices:

- Keep clear and concise records on your organisation's practices as well as any boardroom decisions.
- Conduct a thorough risk assessment along with a health and safety review of your premises and policies.
- Monitor emerging risk areas at the senior level to ensure you can respond to them quickly.
- Update your network security and keep a safe backup of your vital files.

The number of health and safety prosecutions against directors has tripled since the new sentencing guidelines came into force.

The 20 largest health and safety fines in 2016 totalled £38.6 million.

The 20 largest in 2015 totalled £13.5 million.

The 20 largest in 2014 totalled £4.3 million.

CI PROFILE

Crendon Insurance Brokers