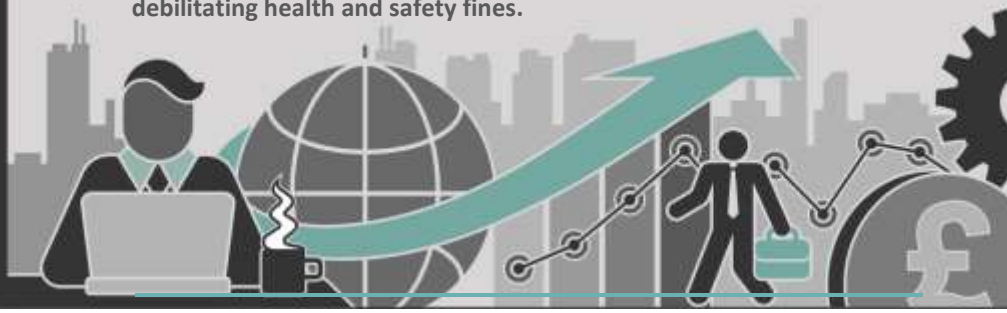
JUNE 2017

CI COMMERCIAL INSURANCE PROFILE

DID YOU KNOW?

According to a new study conducted by health and safety consultants, Arinite, the average cost of a health and safety fine is £75,000 more than the cost of compliance. In general, compliance involves a formal health and safety programme, insurance, and compensation for a designated health and safety employee. Keep reading for more information on how your organisation can remain compliant and avoid debilitating health and safety fines.



IN THIS ISSUE

Crendon Insurance Brokers

D&O Liability for Higher Health and Safety Fines 1 Year Later

In February 2016, the new guidelines from the Sentencing Council came into force. These amendments dramatically increased fines for corporate manslaughter, food safety and hygiene offences, and health and safety offences. Within the first year, the number of health and safety prosecutions against directors and officers have tripled. What's more, is that 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. Research from law firm BLM shows that there has been a 148 per cent rise in the overall amount of fines since 2015, with the average fine amount rising from £69,000 to £211,000.

These new guidelines place a much higher burden on directors and senior managers to ensure that their organisation is compliant with health and safety regulations. If they do not rise to meet this responsibility, the average health and safety fine is £75,000 more than the cost of compliance, according to health and safety consultants, Arinite. Yet, steep fines are not the only deterrent for noncompliance, as it has become increasingly likely that directors and officers could go to prison for either intentional breaches or a flagrant disregard of their responsibilities. In 2016, 34 company directors and senior managers were prosecuted and found guilty, resulting in 12 prison sentences.

To help your organisation avoid these potentially debilitating fines, consider the following best practices:

- Have a health and safety professional conduct a health and safety review of your premises and policies.
- Provide annual comprehensive safe work practices training for all your employees.

However, the most beneficial practice that your organisation can invest in is to purchase robust directors and officers (D&O) cover that also provides run-off cover. For more information, contact the professionals at **Crendon Insurance Brokers Ltd** today.

Nearly Every UK SME Owed £16,000 in Late Payments

More than half of Britain's SMEs were owed an estimated total of £44.6 billion in late payments by the end of 2016, according to recent industry research. That averages out to roughly £16,000 per SME; however, 1 in 10 were owed more than £100,000.

This massive financial delay has been detrimental for affected SMEs, with 65 per cent of them agreeing that late payments force them to shut down. In response, half of all small business owners want the government to intervene and help SMEs overcome these circumstances.

However, your organisation may not be able to wait too long for the government to intervene. For that reason, here are six best practices for handling late payments:

1. **Complete a credit check.** Before you agree to conduct business with a client, you should run a credit check to see whether they may pose a risk.
2. **Make your payment terms clear.** Clearly outline your payment terms, which should include the specific amount due, the date the payment is due and the consequences of not paying on time.
3. **Offer incentives for early payment.** Consider offering a percentage discount on invoices that are settled before the due date.
4. **Add interest to late payments.** If clients do not pay you on time, add interest to what they owe. However, you should only add interest if it has been explained in your payment terms.
5. **Remind clients of pending due dates.** Be sure to contact your clients several months before their due date. If they ignore your notices, remind them if they do not pay on time, they will accrue interest.
6. **Suggest an instalment plan.** If your clients cannot pay what they owe in a lump sum, you may want to suggest an instalment plan.

WannaCry Highlights Why You Should Prepare For Ransomware

WannaCry, a ransomware program that targets a vulnerability in outdated versions of Microsoft Windows, has spread across 150 countries and infected more than 230,000 computers since it was launched on 12th May. It disrupted many NHS hospitals in England and Scotland, infecting up to an estimated 70,000 devices, including computers, MRI scanners, blood-storage refrigerators and theatre equipment.

The danger that the ransomware program poses is based partially on how invasive it is. After infecting just one computer, WannaCry can spread to every device in a network within seconds. It works by locking users out of their computers before demanding money to regain control of their data. Initially, WannaCry requires about £230, but, if no payment is made within three days, it then threatens to double the amount. If no payment is made within that time, the ransomware program then threatens to delete the files after seven days.

Ransomware is one of the most common cyber attacks, accounting for 17 per cent of all security breaches in 2016, according to government research. Even worse, an estimated 54 per cent of UK organisations have been the victims of ransomware. The attack's effects can be quite severe, causing business disruptions, partial or total loss of data, and loss of reputation. To ensure that your organisation is adequately protected from such a cyber attack, consider implementing the following practices:

- Update your network security.
- Install and update anti-virus as well as anti-malware software on all of your organisation's computers.
- Provide your employees with cyber security training. This should include best practices, such as how to recognise a cyber attack.

One vital component of a solid cyber defence is purchasing comprehensive cyber insurance to ensure that your organisation can sustain a cyber attack. For more information, contact **Crendon Insurance Brokers Ltd** today.

CI PROFILE

Crendon Insurance Brokers