



Commercial

INSURANCE SERVICES

insight

Issue 5

How new fire regulations affect you

On 1st October new fire safety regulations came into place that have a significant impact on the operation of your business.

The Fire Safety Order (RRO) 2005 places the emphasis on businesses to prevent fire and reduce risk. It covers nearly every kind of domestic building structure and open place, including:

- Offices and shops
- Premises that provide care
- Community halls
- Common areas of houses in multiple occupation
- Pubs, clubs and restaurants
- Schools
- Tents and marquees
- Hotels and hostels
- Factories and warehouses

The Act also signals an end to Fire Safety Certificates. The onus for complying with the Fire Safety Order now falls on the 'responsible person' on those premises.

It is the duty of the responsible person to carry out a fire risk assessment. This must focus on the safety of all 'relevant persons' in the event of a fire. It must also include consideration for

any dangerous or flammable substances that are likely to be on the premises. There should be special consideration given to individuals at higher risk, such as young persons, the disabled and those with special needs.

Furthermore, the Act extends the area of responsibility to cover individuals in the vicinity of business premises, as well as those on it, in the event of a fire.

Carrying out a Fire Risk Assessment will assist you to identify potential risks and hazards that can be reduced or removed. It will also help you evaluate general fire precautions and identify areas that require improvement.

General fire precautions should protect people against the fire risks that remain, with the nature and extent considered in full to minimise risk. If you employ five or more people you must record your risk assessment and any significant findings. This is however regarded as best practice for all businesses.

For further advice on best practice for complying with the Fire Safety Order call us now.

inside



A Fleeting Risk



Planning for the Worst



Digital Fortress



Better Safe than Sunk



Employers Liability Premiums



A Fleeting Risk

In the UK, one-third of all road traffic accidents involve somebody who is working at the time

Every week 20 people are killed, and a further 250 seriously injured on Britain's roads - many of them carrying out work-related journeys. The following facts also have significant implications for your business:

- 11,897 accidents in a year are fleet and business drivers alone
- Almost one-third of fleet drivers take time off work because of discomfort caused by driving
- Fleet drivers average between 20,000 – 50,000 business miles per year

FACTORS A BUSINESS SHOULD CONSIDER

Work Related Road Safety Policy

If a person is driving on behalf of a business, they are classed to be 'at work'. Both the employer and the employee have a 'duty of care'. In order to comply with this 'duty of care' you will require a Work Related Road Safety Policy.

The main areas these safety policies should cover are:

- Safe driving practices
- Training
- Use of mobile phones
- Breaks and safe driving duration
- Technical safety and roadworthiness

All businesses should have a policy in place for their fleets and with changes in the corporate manslaughter legislation proposed, the need for a Road Safety Policy has become increasingly important. Despite this, 4 out of 10 fleets still have no formal safety policy.

Recommended fleet accident pack

In the event of an accident it is advisable that businesses have some form of protocol for their drivers to follow. This will ensure the correct details are obtained, helping to improve the claims process. The protocol should be communicated to all drivers and should be readily available.

Two methods to use, if a driver is involved in a car incident, are accident checklists and accident packs. Accident packs should include:

- Disposable camera
- Pen
- Paper
- A checklist of information to obtain from the other driver(s)
- Emergency contact details

To get your copy of an accident checklist and for more information and assistance on managing your fleet risks call us now.



Planning For The Worst

Every year nearly one in five businesses suffers a major disruption. Planning for such disruptions is good business practice and is fundamental to the survival of a business.

A disaster could happen to affect both you and your customers. Many businesses which experience a catastrophic event never fully recover, as the following facts indicate:

THE STARK FACTS

- 80% of businesses that suffer a major catastrophe go out of business within 3 years
- 40% of businesses that suffer a critical IT failure go out of business within 1 year
- 90% of businesses that lose data from a disaster are forced to shut within 2 years

THE RIGHT RESOURCES

Forward planning can help avoid many of the pitfalls experienced by businesses following a disaster. This will help you to keep continuity and minimise the disruption for customers and suppliers.

Following a disruptive event, the right resources are required to maintain critical business functions.

These include:

- Sufficient people with the necessary expertise and motivation to lead and manage the organisation
- Access to key records and IT systems
- Reliable means of communication with all stakeholders
- The ability to carry on paying staff and to ensure their safety
- The ability to procure goods and services
- The ability to respond to demands from the media

(www.mi5.gov.uk)

EFFECTIVE PLANNING

Effective planning is the key to disaster recovery and it is vital the following are incorporated:

- A senior member of staff should lead a designated crisis management team
- Succession planning for key personnel should be incorporated
- A robust telephone and/or e-mail cascade system should be organised, enabling all staff to be contacted outside working hours

HELP US PROTECT YOUR BUSINESS

To find out how we can help you manage risks like this, contact us now.

Digital Fortress

With UK crime rates increasing, many businesses across the UK are finding themselves victims of theft and breaches in security. Many present an easy target for thieves as security systems are frequently found to be out-of-date and there is often no set policy to uphold security.

No-one would ever leave their business for the night without locking up and making sure the premises are secure. Yet this, in digital terms, is what computer users fail to do on a daily basis.

The important and commercially sensitive information kept on computers just keeps growing and security often lags behind. This can leave companies open to blackmail from hackers or internet pirates. There's also the threat from revenge by ex-employees – this may come via an IT-based viral attack, or people walking off with laptops containing sensitive information.

How security conscious is your company?

Companies must insist on high levels of security from employees and business partners, checking and monitoring these regularly. Linked systems also cause problems as one weak area of security threatens all those in the chain; wireless access is also a major risk.

Secure systems of work

The modern business faces a wide range of security risks, from physical theft of property to electronic theft of data and information from computer systems. However, it is possible to protect against these threats by:

Security Planning

A comprehensive security and business continuity plan to identify and manage the risks and threats.

Protecting Assets

Physical security to protect your staff and secure information.

Employers have the overall responsibility for the security of their business and simple measures can be taken such as confirming the identity of customers and staff.

Computer systems should be secure and access to them should be protected. If a security breach disrupts everyday business, swift initiation of a contingency plan will allow the company to effectively continue everyday functions.

10 steps to securing your business

One approach that can help you establish an adequate security level is to work to a standard such as BS7799.

This revolves round 10 steps:

- 1 Security policy: Sets out the high level principles a business has in protecting data – creating a document used to educate employees.
- 2 Organisation Security: Deals with the detail of how information security management is organised.
- 3 Asset classification and control: Ensures information and information processing equipment are managed and accounted for as valuable assets.
- 4 Personnel security: Covers any personnel issues such as training responsibilities, vetting procedures and how staff should respond to security issues.
- 5 Physical and environmental security: Looks at physical aspects of security including protection of equipment and information from physical harm.
- 6 Access control: control of access to information and systems on the basis of business and security need.
- 7 Communications and operations management: Examines correct management and secure operation of information processing facilities during day-to-day activities.
- 8 System Development and Maintenance: to ensure security and the maintenance of information integrity.
- 9 Business Continuity Management: ensures the maintenance of essential business activities during adverse conditions, from major disasters to minor local issues.
- 10 Compliance: Concerns business compliance with relevant national and international law, professional standards and any processes mandated by the information security management system.

Better SAFE than



For the average SME, the rules and regulations governing the checking of lifting, pressure or processing machinery can feel daunting.

It is however essential to comply with these. The penalties for not doing so include:

- Fines.
- Prosecution of directors – even corporate manslaughter charges.
- Your insurer has to meet employee claims with no chance of defence.
- Prohibitive rises in the cost of insurance – or no insurance at all.
- Invalidation of your existing cover – leaving you to meet any claim or cost of damage yourself.

Required frequency of checks

Statutory requirements on the frequency of checks have given way to a less stringent, risk-based approach. So the period between inspections can be longer for infrequently-used equipment.

For larger businesses with a plant register, a plant manager and strong control systems, this may be useful, but for most, a more prescriptive approach means less chance of error. The panel below

indicates which plant and equipment needs checking and the recommended frequency.

Unfortunately, the law is constantly changing, which can mean even the most diligent small business could still fall short.

A safer alternative

Independent examination is an approach many companies adopt to minimise the impact of checking.

Today, three or four major specialist companies carry out most of the work. They offer national coverage and all the advantages of economies of scale.

As your broker, with knowledge of your needs and existing insurances, we're perfectly placed to arrange this service. We'll obtain tenders on your behalf, make supplier recommendations, and arrange it so that all inspections dovetail precisely with your existing insurance programme. For more information, just contact us.

STATUTORY INSPECTIONS: FREQUENCY

LIFTING EQUIPMENT

Inspections are required by statute within the specified period, unless a written scheme of examination states otherwise.

Escalators: every six months

Builders hoists: every six months

Cranes and lifting machinery: every 12 months

Excavators: every 12 months

Forklift trucks: every 12 months

Goods lifts and hoists: every 12 months

Passenger lifts: every 6 months

Lifting accessories: every six months

Lorry loader cranes: every 12 months

Motor vehicle lifting tables: every 6 months

PRESSURE SYSTEMS

Inspections required by statute; frequencies are recommended and can be varied by usage or risk assessment

Air pressure plant: every 26 months

Hot water boilers (100°C and over): every 14 months

Refrigeration and air conditioning: every 26 months

Steam boilers and ovens: every 14 months

Steam pressure vessels: every 26 months

Other pressure systems: every 26 months

POWER PRESSES AND PROCESS MACHINERY

Inspections required by statute

Power presses and press brakes: every 6 months

Power presses with fixed guards or enclosed tools: every 12 months

LOCAL EXHAUST VENTILATION

Inspections required by statute

Dust extraction: every 14 months

Fume and vapour extraction: every 14 months

Shot blast units: every 6 months

NHS to push up Employers Liability Premiums

From 2007, the NHS can recover the costs of treating workplace related injuries from an employer under the NHS Cost Recovery Scheme.

In its present cash strapped position, the NHS is likely to make full use of its new powers. Then there's the growth in work related diseases and conditions and the increased awareness by employees of their rights. These factors, coupled with a steady increase in awards, will be the drivers behind an inevitable rise in premiums.

What can I do as an employer?

Put health and safety high on the agenda, as a well run business will pay less premiums in the long-run. We can help by advising you on a range of measures you can take to improve health and safety. For further information please contact us.

