

Managing insurance risks

All businesses face a wide range of risks every day. Careful planning can either reduce these risks to an acceptable level, or eliminate them completely.

While insuring some of these risks is essential, it should be seen as no more than a back-up to an on-going 'risk management' process. This briefing tells you:

- What risk prevention you are required to carry out by law.
- The most common causes of loss or damage, and how to prevent them.
- How to identify the risks your business faces.
- How taking preventative action will affect your insurance policies.

1 Legal requirements

Risk management is not just good business practice. In many cases, it is also a legal requirement.

1.1 Health and Safety legislation requires you to carry out a risk assessment of your business.

You must ensure the health and safety of all employees and visitors to your premises.

(See **Health and safety** and **Health and safety risk assessment**.)

1.2 Taking precautions to prevent injury to employees is a legal requirement.

All businesses must have employers' liability insurance (except those only employing close family or where the owner is the only employee) to compensate employees

who are injured or suffer illnesses through working for them.

- If you fail to ensure employees are adequately insured, you could face criminal proceedings.
- 1.3 Fire regulations** require you to carry out a risk assessment and, in certain instances, to have an inspection and certificate from a fire prevention officer.
- 1.4 Employment law** requires you to follow set procedures when recruiting, promoting or dismissing employees. (See **Employment law: the basics**).
- 1.5 The Companies Act** puts responsibilities on directors of a limited company to protect the assets of the business. (See **Directors' responsibilities**.)

Directors' Briefing

a book in four pages

More than 160 briefings are now available.

If you need further information or help, ask the distributor of this briefing about the services available to you.

Your insurance company will expect you to meet these legal obligations.

2 Premises

Some of the most obvious risks are housed within in a businesses' premises.

2.1 The **main risks** to business premises are from fire, water damage, malicious damage and weather-related damage.

- Electrical faults are a common cause of fires. Ensure that all electrical items and wiring are checked regularly, in line with the Electricity at Work regulations.
- Arson is also a frequent cause. Remove combustible waste, and control access to vulnerable areas (eg warehouses).
- Water damage is mainly caused by burst pipes and leaks from water tanks. Carry out regular inspections, maintenance and repairs.
- Glass is a favourite target for vandals. Glass windows and doors can be made of toughened glass, or protected with grilles or bars, but check you do not require planning permission to install them.
- Flooding and structural damage to your premises can be caused by severe weather. Make sure gutters and drains are cleared and that roofs are kept in good repair. Find out if your premises is located in a flood risk area and sign up for local flood watch warnings. Find tips on minimising flood damage and how to draw up a flood action plan on the Environment Agency website (www.environment.agency.gov.uk).

2.2 Improve **security** systems and procedures.

- Burglar alarms are a good visible deterrent. For reliability, they should comply with British Standard 4737-3.0:1988. The company installing and maintaining them should be approved by the National Security Inspectorate (NSI, 0845 006 3003; www.nsi.org.uk). Insurers will also consider alarms approved by the Security Systems and Alarms Inspection Board (SSAIB, 0191 296 3242; www.ssaib.co.uk). Look for alarms using REDCARE signalling.
- Ensure burglar alarm codes and keys are only available to authorised persons.
- Ensure all telephone line faults are dealt with immediately. The fault could have been caused by a burglar (to disconnect your alarm from the security call centre).
- Make sure all visitors identify themselves and state who they are visiting.
- Appoint a person to check the premises

are secure at the end of each working day.

See **Securing your premises**.

2.3 A professional approach to **managing your premises** will prevent many problems.

- Draw up a list of items which need regular inspection and maintenance. For example, roofs, pipes, tanks and stopcocks are all potential sources of leaks.
- If your premises are liable to flood, keep your stock above ground level.
- Ask your local fire prevention officer and crime prevention officer for advice. Smoke detectors, fire alarms, extinguishers and sprinklers are vital to alert people to danger and to prevent fires from spreading.

If you are a tenant, ensure that your landlord is taking sensible precautions.

2.4 Improve **safety** practices.

- Lock away hazardous and flammable substances in secure storage.
- Ban smoking in areas of the building that contain any flammable materials, such as storage rooms.
- Undertake regular fire drills, so that all employees are aware of the procedures. Keep a log of the timings and results.

3 Equipment

3.1 **Computers** represent a major risk for most businesses.

- Back up all computer data regularly (daily if possible). Store back-up disks off-site.
- Consider installing a back-up or duplicate system. If one computer fails, you can switch to another without loss of data.
- Install an 'uninterruptible power supply', (or, at least, surge protectors). Otherwise, fluctuations or cuts in the power supply can cause loss of data. You may also want to consider getting lightning protection.
- Ban employees from installing software or importing data (eg from a disk) until it has been virus-checked. Computer viruses can wipe out your entire system.
- If you have an Internet connection, consider installing a firewall.

3.2 Any **capital assets** you use to provide or manufacture your product or service should be regularly checked to ensure that they are in full working order.

For example, manufacturing businesses

- should ensure all parts of their production lines are functioning correctly and at their maximum efficiency.
- Equipment failure can mean late delivery, lost orders and cashflow problems.

4 Employees

4.1 The severe impact of the death or illness of a **key employee** can be insured against.

Step-by-step

Use a methodical step-by-step process to identify risks and decide what action to take.

A Identify your key **business processes**.

- For example, a printing firm receives information on disk, lays out the text using a computer, does the print run, then delivers the publication to the customer.

B Identify the **key elements** that make the business processes possible.

- For example, a printing firm needs premises, computers, printing presses, a delivery van, and a team of employees.

C Identify any **strategic threats** that may be worth insuring against.

- For example, litigation is a serious risk for most printing firms, as late delivery of a publication can be disastrous for the customer concerned.

D Run through a list of **common risks**. Check you have not overlooked anything.

E Isolate the most likely **causes** of the risks in **B–D** above. Then take action to eliminate or reduce the risk in each case.

- For example, a printing firm should have fail-safe computer back-up procedures and should take legal advice on how to avoid being sued.

F Decide which risks are worth **insuring** against.

- For example, a printing firm may decide to insure the premises, the computers and the key computer operators.

- Reduce the risk with regular medical checks on key employees.
- Train replacement staff to take over key jobs in the event of illness.

5 Theft and fraud

Many kinds of theft can be prevented by securing your premises. Other threats come from within your organisation and can easily be overlooked.

5.1 Favourite targets for thieves include cash, spirits, clothing, electrical products, cigarettes and computer equipment.

- Indelibly mark all equipment with the company name.
- Some equipment, including computers, can be cabled to desks or bolted down. Your insurance policy may insist on this precaution.

5.2 Theft by employees can add up to large amounts of money.

- Vet all new employees, and especially those who handle money or have access to computer systems. A simple honesty check is to find out whether new employees actually have all the qualifications they claim to have.
- Petty theft is a common problem. Allow only named individuals to order equipment or stationery.

5.3 Collaboration with other organisations can help prevent theft.

- Trade associations and retailer groups often share information on recent thefts. For example, a shop can alert others in its area to gangs of shoplifters.
- Police crime prevention officers can alert you to particular risks facing your business.

5.4 The symptoms of fraud can be undetected until it is too late.

- Set up systems to double-check all invoices and expenses. Employees may submit false expenses claims, inflate invoices from suppliers, or set up fictitious supplier accounts.

5.5 Theft of intellectual property can be even more damaging than fraud.

At times, it is impossible to detect. A competitor may get hold of the information without you even knowing.

➔ To find out more about managing IT risks see **IT disaster prevention and Security and the Internet**.

➔ For information on avoiding bad debts see **Credit control, Debt recovery and Factoring and invoice discounting**.

- Patenting ideas may be too costly for smaller firms, so taking preventative measures is often the best option.
- Restrict access to sensitive information by encrypting computer files. Keep passwords secret and change them regularly.
- Consider taking out legal expenses insurance to help fund any legal battles to defend your rights.
- Consider imposing express confidentiality obligations in contracts of employment.

See **Intellectual property**.

6 Transport

- 6.1** Ensure that all vehicles are regularly **maintained** and that drivers are aware of the legal driving-time limits.
- An accident could mean legal action against your business.
For example, if it is due to faulty brakes, or caused by fatigue because your driver has exceeded the driving hours allowed by law.
- 6.2** Use secure methods to transport **valuables** and other items that might be stolen.
- Your business should recoup the higher costs in lower losses.

7 Insuring the risks

Many business risks can be insured against. But in order to get insurance you may have to agree to take steps to reduce these risks.

- 7.1** Your insurance policy's conditions will normally specify certain security and safety measures which must be in place.
- Failing to comply with these conditions could **invalidate** your insurance. For example, failing to keep your alarm maintained or to keep the code secure.
- Employers' liability or other liability insurance will cover liabilities to others caused by your negligence and may cover failure to meet legal obligations. In extreme circumstances, an insurance company could sue a firm's directors for claims paid by the insurer.
- 7.2** You may be able to reduce your insurance **premiums** by agreeing to increased safety and security measures.
- The fewer claims you make, the less your premiums will increase in the future.

7.3 Consider if some **risks** should remain uninsured.

- For example, the cost of fidelity (staff honesty) insurance may be high for a small business. It may be better to carry the risk and take sensible precautions.

7.4 Some risks are simply **uninsurable**. For example:

- Loss of profits due to the loss or failure of a contract, or due to fluctuations in demand for your goods or services.
- Losses due to shoplifting.

7.5 The **risk management** services offered by many insurance companies, insurance brokers, and industry specialists (eg computer consultants) can often pay for themselves.

By reducing your risks, they can cut your premiums and your claims.

- Risk management will analyse the risks and plan the most cost-effective steps to prevent disaster striking.

7.6 Having a **contingency plan** (or business continuity plan) will help you to recover from any disaster in the fastest time possible.

- For example, how would you cope if your computer system broke down and you lost your software and all your data?

See **IT disaster prevention**.

Further help

There are other Directors' Briefing titles that can help you. These briefings are referred to in the text by name, such as **Health and safety**.

© BHP Information Solutions Ltd 2007. ISSN 1369-1996. All rights reserved. No part of this publication may be reproduced or transmitted without the written permission of the publisher. This publication is for general guidance only. The publisher, expert contributors and distributor disclaim all liability for any errors or omissions. Consult your local business support organisation or your professional adviser for help and advice.