

Risk Management

"It'll never happen to me", amazingly we all believe that bad things happen to others and never to us. Each year many businesses suffer fires or floods or other catastrophes and go out of business as a result. Preparation is the key to survival and all firms should have Risk Management and Disaster Recovery plans in place.

As ever in this type of exercise the major part of the job is defining the risks and removing them or reducing them to manageable proportions. In today's regulated world it is necessary to allocate responsibility and apportion blame and this can only be properly established if each step in the process is recorded. In Health and Safety terms not recording a risk assessment finding and the actions taken to remove or reduce the risk is in itself, a failure.

A common response to an exercise of this type is that managers feel that they know what they are doing and that those working under them are also aware and understand the risks and that nothing will actually change the level of risk. This is seldom the case and often, genuine business benefits can be achieved when procedures are improved. Acceptance of a known removable risk will bring little sympathy or protection to a business if someone is injured or something irreplaceable is lost.

In this paper it is assumed that there is no Risk Management Plan. The guidance applies to all firms irrespective of size and therefore will not consider the statutory requirements, only the practical aspects.

Management responsibility

Risk management must bear the stamp of authority. Set out the responsibilities, starting with the most senior (the Partner or Director responsible) and work through the management / supervision structure of each department. Plan the work to be undertaken by each person. In small firms the Partner / Director may do all the work personally, but at least one other should be involved. Ideally, each firm should have a designated partner who is responsible for risk management issues.

Enter on your Risk Management Plan what you did and when it was done and when it needs to be reviewed.

Insurance

The first check should be to establish the cover provided by any Insurance policies already in place. Update any values, disclose circumstances, take out new policies where necessary. Think about what types of cover are relevant to you - Buildings (boilers, lifts, etc.), people (Employers Liability Insurance or Travel or Personal Accident), Contents (computers and data recovery), Vehicle Fleet, Business Interruption, Key Man and other areas specific to your business. Please also think carefully before rejecting Terrorism cover. Your insurance broker will be able to advise you on what cover is appropriate for your business.

Succession

It seems obvious, but businesses need people so a planned response is needed to deal with their replacement should they leave abruptly. Train under-studies or identify an external person or service which might be recruited or perhaps revise workloads to ensure experience and skills are shared over a number of people. Ensure that the principles laid down are maintained, it's very easy to generate specialists. Using the skilled person as a manager only works if the person is good at delegation, so again the position needs management. The Partner in charge of risk management might also leave, so prepare for this eventuality also.

If you are a sole practitioner and you are taken seriously ill or worse, then your employees and clients will benefit from arrangements put in place earlier by you to protect their interests and papers. Remember that work in progress needs to be identifiable quickly. Computer diaries on hand held computers should be synchronised with desktop computers to ensure they are backed up properly and available. Paper diaries should be done in duplicate, with the partner keeping one copy and his PA / secretary maintaining an office based version.

Partnership Agreements and Conditions of Employment

"Cobbler bairns.....". People don't always follow procedures or understand unwritten rules and particular attention must be paid to Partnership Agreements and Conditions of Employment. Ensure that everyone is clear about what is permissible and what is not. Health and Safety policies are required and assist risk management as risk assessments involve everybody and often highlight office and building maintenance deficiencies more quickly than may have been the case in the past. Today, particularly because of the opportunities offered by technology, businesses are threatened by internal and external sources. Software, E-mail, Internet and computer policies built into agreements and contracts assist in complying with employment law and making it clear to the Partner or employee what is acceptable and what is not. Guidance on this is available elsewhere in the Manual.

Buildings and location

Water leaks and flood-water.

Old water tanks and pipes can do great damage - have a plumber check these. In recent years a great many properties have been damaged by floodwater. If your office is likely to suffer this damage and you can't relocate, plan to base as much necessary paperwork as you can elsewhere in a document storage facility well above the waterline. If this is inconvenient you may decide to scan papers into a computer to allow the papers to be elsewhere without compromising the efficiency of the business. You may also decide to purchase water and fire proof cabinets. File lists detailing the location of each file might be kept at an outside location, otherwise it may be difficult to establish what's been lost. You may decide to do nothing, but again, record what you have done and set a review date if only to check the year-on-year increase of the water level.

Fire

Fire is obviously something to guard against and often this is caused in older buildings by faulty or overloaded wiring. Sometimes lots of computers etc. are added without proper consideration being given to the loading being placed on the system. A poor central heating system can impact your sockets and wiring when numerous powerful electric heaters are switched on. If you haven't done so, have the wiring in your building tested and rewire as necessary. Always consider the increased loading when adding electrical items to your office. Write all of this down and plan a review date.

Ensure fire alarm and emergency lighting tests are undertaken in accordance with the manufacturer's guidance and that evacuation procedures are understood by all parties and staff and fire drills are carried out on schedule. Ensure all of this activity is entered on your Fire Alarm Record, as your local Fire Brigade will want to inspect it.

A Fire Risk Assessment will establish hazards particular to your building and you should make arrangements to correct or repair problems. This Assessment should be filed safely and you should put a bring-forward review date in your diary.

Maintenance

Have a qualified electrician undertake annual Portable Appliance Testing (PAT) as required by the Electricity at Work Regulations.

Ensure gas appliances such as boilers, cookers and fires are tested annually by a properly qualified technician and file the reports.

Security

Are your buildings and car park secure? Are your partners, employees and clients safe from attack within them? Does your Cashier or someone else carry large sums of cash out with your office? Health and Safety risk assessments should have thrown up problems, which can be addressed in a number of ways, such as panic buttons in reception areas, CCTV and good lighting at entrances and in car parks, random timing and routing of banking visits if sums do not justify a security company.

Intruder and fire alarms will probably have been installed but may need review. If your alarm does not link to a monitoring service you may want to consider this as the alarm will be triggered automatically to bring Police or Fire Service attendance therefore reducing the damage caused. If you have any queries regarding security your local Police Crime Prevention office will be able to assist you.

The Police will also give guidance regarding bomb threats, suspicious substances through the mail and other types of attack. They will provide training for Mail Room staff and other mail handlers if asked.

In certain circumstances it may be necessary to protect individuals connected with the firm and also their families and residences. This may be as a result of a recognised threat or as a result of an individual working from home with files etc. which might be

required for this activity, you should operate a 'Key Man' travel policy with individuals on the management team traveling separating whenever possible.

Computer Security

Computers are easily replaceable but lost data can be gone forever. Write a procedure for backing up data daily, weekly and monthly. Backup tapes /disks can become corrupt so it's never a good idea to have only one backup disk or tape. Most organisations use what's called a generation system of backup management to give the best possible chance of recovery. Please ask your supplier for guidance if you are unsure and label all the tapes / disks clearly. Ideally the backup tapes / discs should be tested to ensure the data is being correctly copied onto the tapes / disks and that the data can be read. Do not attempt this testing unless you know exactly what your doing as you may overwrite new data with old. Again ask you supplier to provide training or check the tapes / disks for you. There are also backup systems available on the Internet where data is encrypted and copied to a web server. This is a recent development where an external company takes responsibility for keeping your backup data safe. Terms and conditions should be checked carefully if only to ensure that your data will be available to you should the backup company fail. If your firm has a branch office, arrangements might be made allowing backup from one to be stored at the other or using communications, data can be transferred electronically then backed up at the branch location.

Assuming you are not utilising the Internet backup option, please ensure that backup tapes / disks are stored in a media safe which is specially designed to ensure that the internal temperature does not exceed the safe limit for tapes / disks. Ideally media safes should be located as close to ground level as possible as tapes / disks may be damaged if the media safe in which they are stored falls any significant distance. Always keep one set of this week's backup tapes / disks in another secure location, at home or with your bank or designated dispository. It may not always be possible to access your media safe within an acceptable period if it's buried under the debris of your office. Keep a spare copy of the media safe key off-site too.

Currently, most computer fraud is committed by insiders. Damage can be malicious or just unthinking but again this is mostly caused from within. Ensure data is secure and deny access where necessary. Disgruntled individuals are usually easy to spot but those who wish to steal the contents of a client database or some other data for an ulterior motive are not and the "mole" may stay with you for some time compounding the problem. If you are dispensing with someone's services arrange for their passwords etc. to be deactivated in advance of, or during, the termination meeting.

Unthinking, damage such as copying a screensaver from a disk attached to a magazine may seem trivial but if a virus is attached it can do untold damage. All files added to your systems must be virus checked by a competent person. E-mails with attachments from unknown senders are especially dangerous as is downloading files from web sites.

The Data Protection Act

This Act introduces risks in relation to data held and it is necessary to consider the eight data principles as they relate to your business. It may be necessary for you to ask formally for permission to hold "sensitive" data on a client and to set down procedures for handling "subject access" requests. The Act now requires disclosure of "structured" files (paper in files) as well as data held on computers. Good document management and document retention policies go a long way to reducing the costs and effort of complying with the Act. If in doubt contact the Office of the Information Commissioner, Wilmslow, Cheshire.

Conclusion

This paper is not intended to be comprehensive as firms will have specific problems and nooks and crannies where challenges reside. However the paper should point firms towards identifying, removing, reducing and recording the activity related to general Risk Management and putting in place the thought processes on which a Disaster Recovery plan can be based.

Please keep a current copy of the Risk Management Plan outwith the office and ensure it's available at all times.