# Risk Management Issues

*Expert knowledge means success*

## Contents

# A Business Continuity Plan ...vital for the survival of your business

For most businesses, advance planning for the possibility of a catastrophe will determine whether they can survive should the worst ever happen. A catastrophe may be anything from an IT failure, flood or fire to the illness or death of a key employee - but the key component that marks out the survivors is a Disaster Recovery or Business Continuity Plan. Come the day, those that need one are unlikely to survive without one. These UK statistics tell the story:

- 80% of businesses that suffer a major catastrophe (perhaps serious fire or weather damage) go out of business within 3 years;
- 40% of businesses that suffer a critical IT failure go out of business within 1 year;
- 80% of small and medium-sized company owners admitted in a recent survey that they had no plans in place for dealing with an unexpected event.

Picture the scene, you are phoned at 3am to be told there is a major fire at your premises. You are inevitably upset and, as you arrive, your worst fears are confirmed. Your mind is racing with thoughts about what you will say to your staff and customers. What will happen tomorrow when people start arriving for work and customers start phoning in? But there are no phones to answer! What should you do first? Where will we all go? What is going to happen? If you don't know what needs to happen, customers and staff will leave you and the business will go down fast – that's what!

## Testing Time for Business Continuity Plans

More firms are developing Business Continuity Plans in response to contractual requirement, new regulations or just sound business practice. Once the plan is written, it would be tempting to tuck it away and forget it until the dreaded day when disaster strikes. That in itself could prove disastrous because the plan will gradually fall into disrepair as people, premises or processes change. The plan was written based on circumstances at a point in time and must be refreshed as the organisation evolves. A structured review coupled with regular updating of contact lists is essential.

Testing the plan is also a must because it is the only way of checking that carefully devised contingency arrangements will actually work come the day. By inventing disaster scenarios we can see whether the planned response stands up. Another good option is to watch the press and use the experience of others to check whether the plan would survive or fail. Two recent press stories, one with tragic consequences, were perfect examples.

In March 2004, an underground fire in Manchester damaged telephone cabling and disrupted 130,000 phone lines leaving firms without telephone or e-mail service, some for 2 weeks. Security was compromised for firms with alarm systems monitored via landline, leaving some uninsured. Managers who assumed that telephone breakdowns are always short-lived or that they could muddle through using mobile phones without any real planning discovered just how wrong they were. Isolation from customers and suppliers converted into disruption and business lost, estimated by Manchester Chamber of Commerce at £4.5M each day. The smart ones were those who had planned for just such an event, knew how they would maintain contact and preserve security arrangements.

In May 2004, an explosion at a plastics factory in Glasgow caused 8 deaths, 57 casualties and was a tragedy for the families involved. It stretched the emergency services and many other agencies charged with tackling this most severe of disasters. It instantly affected neighbours, customers and suppliers causing business disruption far from the scene of the explosion. It was also a fatal example to those who see safety management as a bureaucratic imposition that it is actually about people's lives.

What would your story have been if either of these events had occurred on your doorstep?

## Business Interruption Insurance

Business interruption insurance is essential because it provides a financial safety net while the business is recovering, but it takes more than cash to breathe life back into a

business that has suffered a major setback.

Recovery will depend on leadership, good organisation, survival of essential data, documents, and perhaps the ability to maintain production or at least to tell your customers with confidence that you have secured the future. After the event is too late to discover what those plans needed to be.

The process of developing a written plan should answer some obvious "what if" questions like, what if the electricity supply failed? What if we cannot gain access to the building for several days? The answers will lay down the foundations for your plan by detailing who will take charge, what emergency procedures they will follow and what must be in place so that management can steer the organisation through previously uncharted waters.

The benefits of a plan are considerable but, for most managers, writing it will be a new and perhaps difficult project so some help will be valuable.

Your Risk Management advisers should be able to help you in one of two ways. They can source information to help you create your own plan or, if you want to move ahead more quickly, take you through a process of building a framework plan using the latest software tools developed for this task. This first stage can often be completed in one day making it much easier to develop the plan to completion. Plan effectiveness will depend on its scope, clarity and, importantly, a commitment to keep it under review as change takes place within your organisation or trading environment.

Contingency planning is recognised throughout the commercial world as good business practice so it is not surprising that regulators and trading partners, whether banks, insurers or key customers, are increasingly making this a trading requirement. However, there is no mileage in waiting for an outside agency to impose a requirement for something which is basically good for the business. Better to take the initiative and do this in your own timescale. Pick up the phone today and talk to your advisers. If there is a disaster today, that phone might not be there tomorrow!

# Replacement Green Accident Book

The previous yellow book does not comply with data protection laws, as users can read personal information contained in previous entries. From 1 January 2004, all accidents in the workplace must be recorded in a green accident book (BI510) and records must be kept for a minimum of three years.

The green accident book is designed:

- So that any individual recording an accident is unable to access details of previous records;
- To contain basic First Aid information and details of employers duties under RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations);
- To help SME businesses by including a new Introduction to Health and Safety leaflet, so that the emphasis is on preventing rather than recording accidents.

For more information contact HSE Infoline 0845 345 0055.

# Composite Panels

## ...Property Losses

The Association of British Insurers has released its guidance paper on composite panels. This guidance, in the form of a Technical Briefing, provides a risk assessment approach to the fire performance of sandwich/composite panels and takes into account research funded by ABI since 1999 which has been particularly targeted at sandwich panels used internally in the food and cold storage industry. This complements approximately twenty years experience of testing external cladding systems.

The Technical Briefing (downloadable from: www.abi.org.uk/Display/File/78/Sandwich_Panels_Final.pdf) has been written specifically with the needs of insurance surveyors and underwriters but may also be of use to building occupiers and managers.

Other applications present different degrees of risk of inception and fire spread. In interpreting the conclusions of this report for applications other than the above, due consideration must be given to these differences.

Sandwich panels are a building product consisting of two metal faces positioned on either side of a core of a thermally insulating material, which are firmly bonded together so that the three components act compositely when under load (wind-loading, access loads etc). Sandwich panel systems comprise the panels, their jointing methods and the type of support provided.

As with other types of risk, buildings containing sandwich panel systems should be considered on their own merits by underwriters and risk managers, taking account of application, choice of sandwich panel system and fire risk management measures in place. A three pronged approach is necessary, balancing negative factors in any one area with strengths elsewhere.

Sandwich panels do not start a fire on their own, and where these systems have been implicated in fire spread the fire has often started in high risk areas such as cooking areas, subsequently spreading as a result of poor fire risk management, prevention and containment measures. Prevention of ignition and containment of early fire spread are critical. Specific and detailed risk assessment is crucial. Where high levels of risk management are not achievable, due to the nature of the processes in the business in question and/or the quality of the management demonstrated, and the risk of ignition is high, the use of panel systems with high fire performance characteristics should be considered. Systems meeting accreditation schemes such as LPS 1181 demonstrate such characteristics.

Some applications, including stand-alone cold stores and panel systems used as external claddings in areas where arson risk is low, have experienced few fire losses. In low risk situations such as these there can be greater flexibility in choice of panel system, taking account of other business needs such as hygienic environments and insulation properties.

Inevitably many situations will fall between clear cut ‘high’ or ‘low’ risk scenarios. Here the degree of financial exposure is likely to drive insurers’ decisions. Fire stop panels and other fire safety management measures have a significant role in such situations, and the importance of a demonstrated ability by facilities managers in ensuring that such systems are robust cannot be over-emphasised.

# Mobile Phones

A new offence came into force on 1 December 2003, banning the use of a hand-held phone whilst driving a car. The penalties are as follows:

- A maximum £60 penalty;
- A maximum fine of £1000 for cars and £2500 for goods vehicles or passenger-carrying vehicles with 9 or more passenger seats and buses, if the driver is taken to court;
- The addition of 3 penalty points, or disqualification at a court’s discretion.

Several studies have shown that drivers who use hands-free kits are just as distracted as those who hold phones in their hands. However, the Government felt that there would be considerable difficulty in securing a conviction against someone using a hands-free kit, and the mobile phone industry had lobbied strongly against banning such devices. Doing so may well have criminalized the six million motorists who had been encouraged to purchase such kits!

Employers are still strongly advised to make it a disciplinary offence for an employee to use a mobile phone whilst driving on business. Failure to do this could lead to a company facing action under health and safety laws if the worker has an accident.

Certain issues have been clarified:

- Holding the phone on a shoulder or getting someone else to hold it to the ear will be an offence;
- Pushing buttons while the phone is on a cradle, lap or on the seat is not prohibited under the new laws but may constitute not having proper control of a vehicle, particularly if it results in an accident;
- Drivers sitting stationary in long traffic jams with the engine running will be allowed to make calls, but this would not mean while stopped at traffic lights for instance.

The HSE has produced guidance for employers on road safety. It can be viewed at www.hse.gov.uk/roadsafety/report.htm

## Mobile phones in cars…….an Update

As mentioned, it is now a criminal offence to use hand-held mobile phones whilst driving. It is also an offence to "cause or permit" a driver to use a hand-held mobile while driving - so the Department for Transport has warned that companies should issue clear guidance to their employees. ROSPA recommends that employers adopt a formal policy on driving to include the following points:

- Employees should never be required to be available on mobile phones while they are driving;
- Making and receiving calls whilst driving should be prohibited;
- Checking for messages and dealing with calls should only be done when the vehicle is parked;
- The message facility should be activated before commencing a journey;
- Risk assessment of driving and vehicle use including checks for and limits to using the car as a mobile office. (The HSE guidance document entitled "Driving at Work", specifically calls for employers to avoid situations where employees feel under pressure).

Breaches of these guidelines by employees should be a matter for disciplinary action.

# Flexible Working

## … parent-friendly policies at work

Recent surveys suggest that employees value time and flexible working more than any other conditions, including pay! So what do we mean by "flexible"?

- Job sharing;
- Compressed working hours;
- Annual hours working;
- Term time working;
- Homeworking;
- Extended leave;
- Flexible working hours.

Since April 2003, an employee with parental responsibility for a child under 6 or under 18 if disabled, has a right to request flexible working. This applies to businesses of all sizes. Employees must have completed 26 weeks service to qualify and make their request in writing, explaining the effect that the change would have on the employer.

The employer then has 28 days to arrange a meeting to discuss the request and then he must notify the employee of the decision within 14 days of the date of the meeting. The employer may have good reasons to refuse the request:

- Short-staffing problems;
- Safety reasons – for example, other staff being left on their own;
- Inability to meet customer demand;
- Burden of additional costs;
- Negative impact on quality or performance;
- Not enough work during the time when employee proposes to work;
- Planned structural changes within the company;
- Any other grounds specified in the Regulations.

The overall thrust of the new law is to encourage fruitful and positive dialogue between employer and employee, and to encourage good working practices. In reality, it may be far easier for large employers to carry out flexibility than SMEs. BIS supply forms that can be helpful in guiding the parties through the process and these can be found at www.bis.gov.uk/er/workingparents.htm

# Measuring Stress in the Workplace

Latest absence figures show that more time is lost due to stress than any other cause. In 2004, nearly 600,000 employees took time off due to stress, resulting in the loss of 13.4 million working days. Recently a hospital was issued an enforcement notice for failing to protect doctors and nurses from stress at work, and giving them a target date to measure and reduce the levels experienced by staff. Even trade unions focus increasingly on work/life-balance issues.

In order to meet the new standard, you will need to carry out a risk assessment to identify the hazards that cause stress. Common causes include:

- Excessive hours;
- Bullying and harassment;
- Poor scheduling and management of workloads;
- Badly designed working environments;
- Inadequate support for staff from managers;
- Failing to give employees sufficient authority and discretion in how they do their jobs.

# Data Protection

## Do you know your obligations?

The Data Protection Act 1998 restricts the use of personal information held on computer and paper. Its safeguards are intended to ensure that data is processed fairly and lawfully, secured and updated by the employer. Individuals also have rights to access the records held on them. However, many businesses are often unclear about how the Act should be applied in real workplace scenarios. What do small firms and organisations have to do?

Registration with the Information Commissioner is the first step. The employer must declare where data is being held, for what purpose and how it is secured. Access to confidential data must be controlled including physical security of paper records and passwording of computer files. Safe disposal of data is also essential so investing in a shredder is a must. The data must also be reviewed to make sure that it is current and accurate.

Employers should be aware of employees' rights of access to their records. Their requests must be made in writing and a recent case, Durant v Financial Services Authority, issued guidance on employees' rights and what data falls within the scope of the act.

Personal Data must name or directly refer to an individual and focus heavily on the individual. The fact that an individual's name appears on a document does not mean that it contains personal data about them. The employee's right of access is to determine the accuracy of the data only, not for troublemakers to fish for information to make claims against the Employer.

For more detailed information, please contact us.

# E-mail Signatures

## Why have them?

As use of e-mail has developed, so has the practice of adding a standardised signature for the organisation. Some have an element of advertising in mind and some have a full page of disclaimers which nobody in their right mind would read when they accompany a one-line message. The law on this area is not entirely clear but there are some basic rules to follow in the interests of security and good practice.

As with printed letters, an e-mail should clearly identify the sender. Limited companies should include the same information as they would on printed letters including company name, company registration number, registered office address and any regulatory information.

It would be wise to include a statement that the e-mail is confidential, only intended for the addressee and that any opinions expressed are personal and not those of the sending organisation. The intention is to protect the organisation against a breach of confidentiality or a claim of libel; a worthy intention but of uncertain effect. These aspects need to be addressed in the organisation's E-mail Policy and HR rules if they are to have any impact.

The inclusion of a signature or a house style may help you to demonstrate that a virus purporting to have come from your e-mail was actually relayed from someone else's computer that just held your e-mail address.

Whether or not the inclusion of tiresome and lengthy disclaimers would influence a court is hard to measure. When e-mail is meant to be a quick means of communication, would a court reasonably expect you to have read and complied with a full page of blurb accompanying a one-liner? Doubtful!

A website that covers this subject in detail is www.emaildisclaimers.com

## Practical management of the risks of work related stress

There are practical things that organisations can do to manage the risks associated with work related stress.

The HSE's Better Working Environment Division (BEWD) produces advice and publications in the form of guidance, standards and regulations on work-related ill-health matters including stress. Their action pack *Real Solutions, Real People* can be used to develop solutions to manage these risks. The pack includes an introduction on how to use it, learning points, prompt cards, and an action plan to record and monitor what needs to be done.

For further information see our publication *IP627 – Stress at Work* or visit www.hse.gov.uk/stress

# CHASPI - A Statistical Service for Businesses and Insurers

Faced with the recent dramatic rises in their Employers Liability insurance premiums, businesses have a strong commercial motive to audit their safety performance and safeguard the relationship with their insurers. A new initiative sponsored by the HSE is designed to help them do that.

The Corporate Health and Safety Performance Index (*CHaSPI*) allows firms to log their accident statistics on a public site which can be viewed by other businesses in the same sector for comparison. Initially it is only for organisations with more than 250 employees but a version for the SME sector is already under development.

Firms presently remain anonymous but it is expected that they will be identifiable after the validation process of this new venture. Logging of information is voluntary but, when management of safety is set in a culture of greater transparency, accountability and social responsibility, the good employer will see this as an opportunity to advertise their safety credentials. Employers who choose to keep their information confidential may achieve negative advertising by default.

For more information go to the development site www.chaspi.info-exchange.com

# Site Security

In April 2003, the Security Industry Authority (SIA) was launched in response to the Private Security Industry Act 2001. One of the SIA's functions is to license individuals in specific sectors for their security activities and to approve security companies. For example, a Company guarding a building site must hold a licence and pass a record check, which needs updating every five years. A contractor is no longer able to use a labourer as a "gateman".

The licence fee is £190 per person for a three year licence (August 2005) and each individual will be required to pass a recognised training course. For more information, visit www.the-sia.org.uk

# Asbestos Management

## The Deadline has passed but are you in the clear?

In May 2004, the deadline passed for "duty holders" of buildings to identify whether and what type of asbestos is present and to put a management plan in place to control the risks found. The regulations required an asbestos survey carried out by a "competent person" and the results, including the description and condition of the asbestos, recorded in a register for the building. Maintenance personnel and contractors must be made aware of the asbestos information before carrying out any work which might expose them to the asbestos.

Firms and individuals that have failed to act are already breaking the law and will increasingly run into a heap of trouble with enforcement agencies, insurers, valuers and contractors whenever maintenance, alteration or demolition work is commissioned.

If you have not acted during the 18 month lead in to this law or are unsure whether you are a "duty holder" find out about your obligations under the Control of Asbestos at Work Regulations by visiting www.hse.gov.uk/campaigns/asbestos/index.htm

# Waste Management

## Waste Electrical and Electronic Equipment Directive

The Waste Electrical and Electronic Equipment (WEEE) Directive aims to reduce the waste arising from electrical and electronic equipment and increase its reuse, recovery and recycling. The Directive applies to all those involved in manufacturing, selling, distributing, recycling or treating electrical and electronic equipment. The equipment covered by the directive includes:

- household appliances;
- IT/Telecommunications equipment;
- audiovisual and lighting equipment;
- electrical and electronic tools;
- toys, leisure and sports equipment;
- medical devices; and
- automatic dispensers.

The Directive aims to address the environmental impact of electrical and electronic equipment and to promote its separate collection when it becomes waste. WEEE is a priority issue for the EU because of its growing volume in the municipal waste stream and its potential hazardousness following disposal.

The Directive introduces producer responsibility for waste electrical and electronic equipment (WEEE). Producers will have to finance treatment and recycling/recovery of separately collected WEEE in the UK to specified treatment standards and recycling/recovery targets. Retailers have an obligation to offer take-back services to householders. The Directive does not place any obligations on householders, and they will not be prohibited from throwing WEEE away with general domestic rubbish. It will however encourage more WEEE to be reused or recycled by ensuring that there is a network of facilities in place where householders can return their used equipment free of charge.

The Department for Environment, Food and Rural Affairs (Defra) is warning companies disposing of equipment covered by the Directive that they may be in infringement of this new hazardous waste legislation. It will introduce regulations that cover the treatment permitting requirements of the Directive.

Regulations to bring the Directive into law were originally due in summer 2005 and imposed a deadline of 13 August 2005 for implementation of its obligations on producers and retailers. However, practical difficulties in meeting the deadline resulted in the Directive's producer responsibility obligations for household and non-household WEEE and its take-back obligations on retailers and distributors to be delayed until January 2006. Further delays followed, and a final consultation and implementation timetable was announced on 25 July 2006 by Malcolm Wicks, the Energy Minister.

Launching the Government's consultation on the key proposals to be introduced from 1 July 2007, Mr Wicks said:
*"Electrical equipment is the fastest growing category of rubbish across the European Union, with around 20 kg per person produced every year, and the UK alone is now generating around 1m tonnes of the stuff every year."*

The consultation marks the beginning of the final phase of the Government's process for implementing the WEEE Directive and can be viewed at www.bis.gov.uk/consultations/page32448.html

The key proposals are:

- A national Distributor Takeback Scheme which will establish a network of Designated Collection Facilities enabling consumers to return their used items for recycling or reuse;
- Obligatory registration for producers through approved compliance schemes;
- Authorised Treatment Facilities, which will process WEEE and provide evidence to producers on the amount of WEEE received for treatment;
- Accredited reprocessing/recycling facilities who will provide evidence of reprocessing to producers;
- An end-of-year settlement to ensure producers are able to meet their obligations via an "Exchange system;
- A voluntary approach for producers to show the cost of handling historical WEEE.

The BIS[1] has published an implementation timetable showing the significant milestones for distributors and the operators of the distributor takeback scheme and designated collection facilities, as follows;

- BIS tender for the operator of the national distributor takeback scheme in parallel with the Consultation on the WEEE Regulations in third quarter of 2006;
- BIS to make provisional appointment of the operator of the distributor takeback scheme in Autumn 2006;
- WEEE Regulations apply from January 2007;
- Formal appointment of the operator of the distributor takeback scheme shortly thereafter in January 2007.
- The operator of the distributor takeback scheme will then recruit members. If you intend to join the DTS, you should submit registration data before 31 March 2007;
- Designated collection facility upgrade and approval from January until June 2007;
- Under partial producer responsibility household WEEE containing Ozone Depleting Substances (refrigerants), Cathode Ray Tubes and Gas Discharge Tubes will continue to be collected through local authority civic amenity sites until 30 June 2007. Other household WEEE need not be collected;

### WEEE and RoHS guidance

Envirowise is a practical environmental advice resource programme for business, managed for the Government by Momenta. They produce the following guides on the WEEE and RHOS legislation:

- Actions you need to take.
- A guide to marketing, product development and manufacturing actions you need to take.
- A guide for the sustainable design of electrical and electronic equipment for compliance to legislation.

Source:
http://envirowise.wrap.org.uk/

- Distributors must provide information about these partial collection arrangements from 1 April until 30 June 2007;
- Designated collection facilities and in-store takeback must operate from 1 July 2007 for all WEEE, at which point the DTS must operate a viable network of out-of-store DCFs, and distributors who have not joined the DTS must offer in-store takeback;
- Distributors must provide information about EEE and WEEE from 1 July 2007;
- Producer compliance schemes are responsible for clearing separately collected household WEEE from DCFs from 1 July 2007.

The WEEE Directive can be viewed at www.bis.gov.uk/files/file29931.pdf

### Restriction of the Use of Certain Hazardous Substances Directive

The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RHOS) Regulations came into force on 1st July 2006. This Directive bans the placing on the EU market of new electrical and electronic equipment containing more than agreed levels of lead, cadmium, mercury, hexavalent chromium, polybrominated biphenyl (PBB) and polybrominated diphenyl ether (PBDE) flame retardants.

Manufacturers need to understand the requirements of the RoHS Directive to ensure that their products, and their components, comply. More information is available from www.rohs.gov.uk

### Non-hazardous landfill waste

From 30 October 2007 new rules apply for non-hazardous waste. Liquid wastes are banned from landfill and other waste must be treated before it can be landfilled.

The Landfill Directive sets demanding targets to reduce the amount of biodegradable municipal landfilled waste and aims to reduce the pollution potential from landfilled waste that can impact on surface water, groundwater, soil, air, and also contribute to climate change. It is applied under the Landfill (England and Wales) Regulations 2002 and must be fully implemented by July 2009.

If you are a business that produces any waste you may be affected. Your waste collector, or the disposal site you take your waste to may ask you to do things like separate recyclables. For more information visit www.environment-agency.gov.uk/landfilldirective

## IT Security – Wireless Threats

### Security of laptops and backup media

There are more than 1 million wireless networks in the UK but half of these operate without even the most basic protection from hackers. A sophisticated snooper, equipped with a laptop and free software downloaded from the internet, can access confidential data in unprotected computer systems. He/she need not even be on your premises if the wireless range extends into your car park or an adjacent road.

Whilst maintaining a sense of perspective over the level of this threat, network security definitely opens up new opportunities for the determined hacker and even businesses with no wireless network could be vulnerable. Most laptops, hand-held computers and mobile phones are now sold wireless-capable so, even if connected to your network by wire, unauthorised connection to another wireless device could be enabled.

Business travellers who use free wireless networks in coffee shops, airports and railway stations need to take special care. When logged onto a wireless network, access permissions to the laptop must be set to deny unauthorised entry. In other environments, there might be a working requirement for shared access so different security levels are needed when accessing a public wireless network. Businesses that require remote working should ensure that IT security procedures are consistently applied out of the office.

A leading global provider of security and control products has a three step approach to protecting wireless networks. It is detect, secure and control:

- Detect all the wireless activity inside and outside your premises. Without round the clock scanning, you cannot know who is connecting to your computer network;
- Secure your data against hostile activity, theft and manipulation. This can be as simple as turning on your hardware and software's built in security capability;

- Control your network with security policies that are appropriate to the wireless age. For example, prevent staff connecting their own equipment to the network, thus compromising your IT security. Security measures need to be continually monitored for effectiveness.

The laptop computer has revolutionised work to the benefit of mobile staff but it is potentially the weakest link in the hardware security chain. Executives, whose laptops are likely to hold the most sensitive information coupled with the greatest functionality in terms of drives and internet access, would do well to check that they are following the most stringent security measures.

Security of backup media is another area of concern, especially when the backup process utilises a tape or disk and is undertaken without sufficient attention to the privacy of data held on the backup media. The computer which generates the back-up may have layers of access control but the back-up media is unlikely to be passworded so security of the storage location is crucial. On-site storage looks attractive because managers can easily control storage but this comes with the inherent concern that the data is exposed to a premises catastrophe. Use of a media cabinet reduces but does not eliminate this risk and any situation which prevents access to the premises will also prevent access to the back-up data with consequent delay in restoring the IT function to another location. Off-site storage is therefore generally considered to be the better practice but it still calls for an appropriate level of security at the storage location. Disturbingly, it is not unusual for backup media to reside overnight in someone's car. Do you know whether your backups are safely stored?

# Health & Safety - Work at Height

The Work at Height Regulations 2005 came into force on 6 April 2005. They consolidate previous legislation and implement the EU Temporary Work at Height Directive. They cover, with very few exceptions, all employers and the self-employed in all industry sectors. The Regulations place obligations on employees whenever there is a risk of a fall liable to cause personal injury – with the exception of sports, recreation and team-building. They are far wider in scope because of the removal of the previous 2-metre rule imposed by the Construction Health Safety and Welfare Regulations 1996. Those regulations required employers to provide suitable edge protection and fall prevention measures for work at or above the 2 metre level. The principle established by the Health and Safety Commission (HSC) in developing the new regulations is a goal-setting one requiring the most appropriate measures to be selected in all cases where there was a risk of falling a distance liable to cause personal injury.

Falls from height are the greatest cause of workplace fatalities and the second greatest cause of major injuries. Around 70 workers die and 4,000 are seriously injured each year in the UK.

Falls from height occur throughout industry and there are two main categories of fall:

- High falls (over 2m) which occur most frequently in the construction and agriculture sectors;
- Low falls (less than 2m and not including slips or trips at ground level) are shown to be particularly common in the Manufacturing and Service Industry sectors.

Whilst falls from height account for the majority of fatalities and also cause a significant number of major injuries, falls at lower levels are the greater in number. They are also the most significant cause of working days lost through injury. Low falls average over 3,500 per year and each will typically result in 1 or 2 days off work.
The new regulations set out obligations on employers for organisation and planning, assessing competence and training of employees as well as assessing and avoiding the risks of working at height. Additionally, the regulations cover the selection, requirements and inspection of work equipment and establish the need for inspections of places of work at height.

The HSE website that covers this subject in detail is www.hse.gov.uk/falls

# Online Banking Fraud

## Top tips to prevent loss

The undoubted convenience to small businesses of online banking facilities should be weighed carefully against the risk of compromising security. Businesses should

expect to use internet banking with complete confidence but intelligent management is vital to keep funds and business information secure. The first steps might be to check that your bank takes internet security very seriously, that you can comply with its online banking guarantee and also that it offers regular advice on maintaining security. Next there is an absolute need to put basic security procedures in place. The following tips were recently published by a leading internet security organisation:

- When logging on to the internet be aware of your surroundings. If you are using a computer in a public place can you be overlooked? Make sure you are not using equipment that would allow electronic eavesdropping;
- Ensure your bank uses encryption technology;
- Whenever accessing your online bank, always type the URL into your browser;
- After log-in double-click on the padlock symbol to ensure the site certificate belongs to your bank;
- Do not open attachments in e-mails unless you are absolutely sure you are waiting to receive that particular file. Always check suspicious e-mails and be wary of any asking for financial information;
- Keep your PC operating system up to date and update your anti-virus software frequently;
- Use firewall software and install software to detect and remove spy ware;
- Do not use the same password for all your online accounts;
- Do not store online account information and passwords in files held on your computer;
- Always log-out correctly.

More information is available from www.banksafeonline.org.uk

# Identity Fraud

## Lessons for business

Identity fraud is the UK's fastest growing crime and there are important implications for businesses, not least the mental strain on victims who become embroiled in the task of purging this crime from their lives. Business executives are natural targets because of their higher earnings and credit ratings. The resultant distraction for any victim is bound to affect attendance, performance and, for the owner/manager whose personal and business affairs may be inextricably linked, the financial implications could be very serious. For personal security, document shredding is now as important as good house locks. For business, paper shredding should already be standard procedure to secure confidential data and meet Data Protection Act requirements. However, many firms operate at less than an acceptable level of security and they may be your trading partners. As part of any security review, you may want to go beyond the implied security of the Data Protection Act and check the data security procedures of suppliers and advisers.

Valuable information on how to avoid becoming a victim is available from www.cifas.org.uk

# Property Arson

## Neglected measures

Insurers acknowledge that arson is the biggest cause of fire and yet risk management programmes often place the greatest emphasis on trade processes instead of arson prevention. There is some practical advice for SMEs available from the Arson Prevention Bureau (APB) which is an insurance industry funded unit within the Association of British Insurers. The following points are extracted from the APB's 24-point plan to increase your protection against arson:

- In any enterprise the owner/manager or a named individual of senior grade must be made responsible for fire safety including protection from arson attack;
- Think about the ease with which intruders/arsonists could break into the premises and take immediate steps to strengthen your defences;
- If there have been any small fires on your own or neighbouring premises inform the police immediately as well as calling the fire brigade. A small fire could be a warning of something worse to come;
- Letter boxes should have metal containers fitted on the inside;
- Stored material of any kind should not be stacked adjacent to fences or walls where it could be set alight from outside;
- Combustible material should not be stored close to the exterior of a building. A distance of 5m is desirable or, if not possible, 3m as a minimum. Skips should also be at a similar distance or, if not possible, lidded skips which are secured daily could be a suitable alternative;

- A named individual must be responsible for securing the building and site at the end of each working day.

The full plan and other information on this subject is available from www.ukfiretraining.com/inp/view2.asp?ID=28

## Further Information

The information in this publication is for general guidance only and is not intended to replace specific advice whether legal or otherwise. Users should verify that any procedure adopted is suitable and sufficient for their purpose and does not breach any law or right of employment whether statutory or contractual. Users of this information do so at their own risk on acceptance that the publishers cannot be held responsible for any loss or liability alleged to have arisen from its provision.

References:

[1] The Department for Business, Innovation & Skills (BIS) was formerly known as the Department for Business, Enterprise and Regulatory Reform (BERR) and before that was called the Department for Trade & Industry (DTI).




Publication issued or updated on: 1 December 2007

Ref: 640