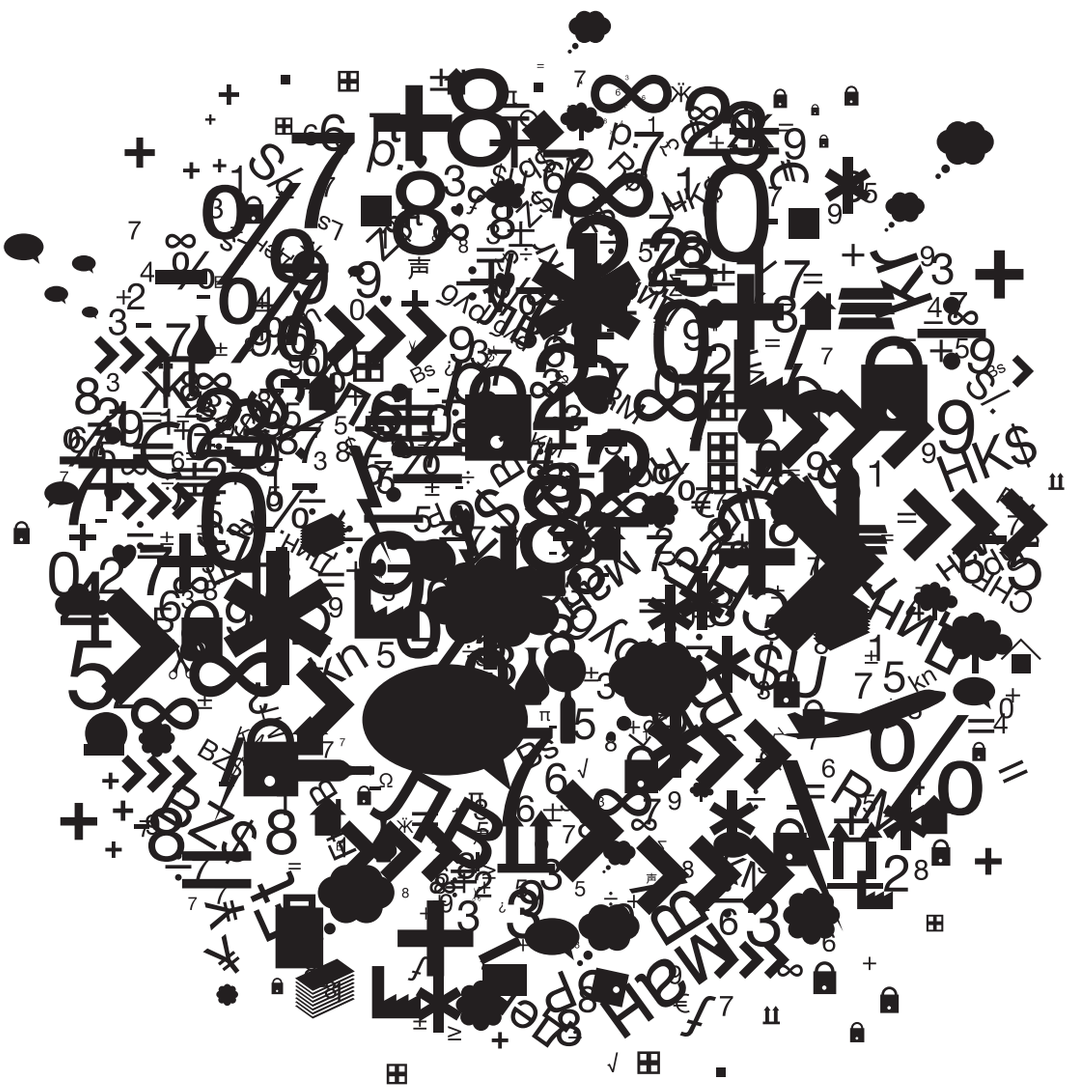
Strategic RISK
www.strategic-risk.eu
[November 2011]

Risk management for mid-sized companies

A detailed report on emerging risks, helping you go a step further than your peers, to outperform them and reap the rewards

XL Group
Insurance
Reinsurance



Properties, transport, energy, art, manufacturing, insurance, aerospace, contracts or people.
Whatever your world is made of, we're here to help your business move forward.

MAKE YOUR WORLD GO

xlgroup.com

Foreword & Contents

WELCOME

THIS '*STRATEGICRISK* LITE' PUBLICATION IS DESIGNED TO EDUCATE UK middle-market companies (those with a turnover of between £50m and £500m a year) about risk management issues and the solutions available.

Most companies of this size do not have a dedicated risk manager who is responsible for buying insurance and educating the business about risk management. In addition, they may not have sophisticated business continuity, business resiliency and enterprise risk management systems.

There is, however, increasing pressure on these organisations – mainly through business relationships and supplier agreements with larger companies – to improve their risk management.

Sue Copeman is editor-in-chief of StrategicRISK

SOMETIMES IT MAY SEEM THAT THE ODDS ARE STACKED AGAINST MID-SIZED COMPANIES, AND in favour of their larger competitors. But there are some advantages to not being huge.

Mid-sized companies are often nimbler when it comes to responding to changing market conditions and new demands, for example. They can also learn from the successful strategies adopted by big organisations – in particular, benefitting from tried-and-tested risk management strategies, designed to save money, reduce losses and improve performance.

You probably have a fair understanding of your basic risks: property damage, business interruption and liability. This guide is designed to help you move a step further: looking at emerging risks, or existing risks growing in importance, for which good risk management can make a significant difference in terms of reducing potential losses and outperforming your competitors.

If you do not have large financial resources, it is likely that you buy insurance to cover only those risks that you consider could really harm your business. At the very least, having good risk management will ensure that you pay less for this cover than your less savvy competitors. If your risk management is truly excellent, you will be able to distinguish between those risks for which insurance is vital and the low-frequency/low-impact risks that you can afford to self-fund, again minimising your insurance costs.

We are committed to helping mid-sized policyholders prosper and implement the strategies that can help them build a robust business.

Denis Burniston, chief underwriting officer, UK middle market, XL

Editor Nathan Skinner
Editor-in-chief Sue Copeman
Market analyst Andrew Leslie
Group production editor Áine Kelly
Deputy chief sub-editor Laura Sharp
Business development manager Donna Penfold
tel: +44 (0)20 7618 3426
Production designer Nikki Easton
Group production manager Tricia McBride
Senior production controller Gareth Kime

Head of events Debbie Kidman
Events logistics manager Katherine Ball
Publisher William Sanders
tel: +44 (0)20 7618 3452
Managing director Tim Whitehouse

To email anyone at Newsquest Specialist Media, please use the following: firstname.surname@newsquestspecialistmedia.com

SPONSORED BY

XL Group Insurance Reinsurance

Know your own appetite

Mid-sized companies seeking to survive and grow need a competitive edge. You have to be able to demonstrate that you are managing your business better than your peers, and that means taking on risk as well as guarding against it

KEY POINTS

01: Good risk management gives you a stronger base to defend your other management decisions.

02: Knowing and managing your risks also provides financial benefits, as insurance premiums will be lower if you demonstrate efficient systems.

03: Insurance is a vital part of your toolkit and brokers need to know your appetite for risk to provide the best cover.

04: Map your risks in order to see where possible weaknesses lie.

05: Investors' and customers' attitudes to risk should steer your strategy as much as the board's.

ALL BUSINESSES TAKE RISKS. Successful businesses take calculated risks. Good risk management has a central part to play in ensuring that your business does not take on more risk than it can cope with or so little that it misses out on opportunities.

There is a common misconception that risk management centres around negatives – preventing bad things from happening and making investments that are hard to justify.

It is true that it is hard to prove the value of risk management designed to protect your business if there are no problems. For example, should you have installed an expensive sprinkler system if you have never had a fire?

But good risk management is actually just about good management in general. If you manage risks well, you can make informed decisions, secure in the knowledge that your business is protected.

You can defend those decisions if stakeholders question them, you can put up a robust defence against allegations from employees or members of the public that you have been negligent, and you will not be caught out if an unforeseen event disrupts deliveries from a major supplier. Essentially, you are working from a better business base than you would be if risk management were absent.

Good risk management can also produce some concrete financial savings. For example, absence management can substantially reduce the costs to your business arising from employees' sickness.

Your insurance premiums will be lower if you can demonstrate efficient controls and systems.

Where insurance fits in

Good risk management is not just a matter of buying insurance. But insurance is an important part of your risk management toolkit, as it protects your company against business-threatening risks. Therefore, understanding what to insure and how much to insure it for is crucial.

To make appropriate risk management decisions, you need to consider not just the board's attitude, but also that of your investors and customers

An insurance broker's help is valuable when making these decisions. While you may just consider one business and one set of risks, brokers deal with a large number of companies. They can provide constructive risk management advice based on their breadth of experience and will know the markets that can give you the best cover at the most competitive price.

Your broker should act on your behalf and obtain competitive quotations from a number of insurers. Your broker should also be able to indicate how your risk management and performance compares with that of peer companies, enabling you to benchmark your progress.

In order to work most effectively with your broker and achieve the optimum result from your insurance-buying strategies, you need to evaluate your risks and understand your company's appetite for risk. Just as some people are prudent and others are gamblers, companies' attitudes towards risk vary.

Evaluating your risks

A structured approach to risk management requires you to evaluate and prioritise your risks. There are many ways in which you can do this, but perhaps the simplest is by drawing up a risk chart or map. This should include all the risks that your company might face, graded according to likelihood and severity of impact.

Input from all parts of the company is valuable here. What some departments perceive to be high risk, boards might not consider major threats. There may be common risks that your business units face, the impact of which individually might not be severe, but could pose a major problem cumulatively.

For example, individual units may be using the services of a single organisation, perhaps in connection with IT or plant maintenance. Each may have limited exposure should that organisation fail, but the cumulative effect could be major disruption for your business.

Mapping your risks allows you to categorise them. You can identify the high-frequency, low-impact, low-cost risks that you should consider self-insuring. Transferring them to an insurer may not be worthwhile. The premium you pay will take account not only of the steady stream of claims payments that the insurer will have to make, but also its administrative costs and profit margin. It may be more

cost effective to fund these in-house and employ appropriate risk management strategies to diminish them as much as possible.

Your risk map will also highlight unlikely but very high-impact risks, over which you may have little or no control – for example, an aircraft crashing into your head office. These may be worth insuring against, as the premium charged should be low, reflecting the remoteness of the event.

In the middle, the medium-severity/medium-likelihood range will include a range of risks. You need to consider how applying risk management can affect their rating and make a decision as to whether or not to insure them.

How much do you take on?

Risk appetite – how much risk your business feels comfortable in taking – is not just a matter of your company's financial circumstances. In order to make appropriate risk management decisions, you need to consider not just the board's attitude, but also that of your investors and customers. Risky strategies can save money in the short term, but can be expensive if things go wrong.

For example, if you are producing or storing goods, it may be cost-effective to focus this on a single site. But, if those premises are destroyed, say by fire, would you have a lengthy period of business interruption, during which customers would be lost?

Similarly, you may have a 'just in time' delivery strategy from your suppliers. Again, this can save costs. But, if a disaster hits an important supplier, do you have any back-up producers that you can turn to or sufficient supplies to meet demand while that supplier recovers? Would your customers be happy to continue buying from you with the potential threat of disrupted deliveries?

Establishing your company's risk appetite is important. It will govern how much insurance you buy and factors such as the size of your chosen deductibles – the first amount that your company pays towards any claim – in insurance policies,

The Institute of Risk Management published its *Risk Appetite and Tolerance* guidance paper in September 2011 to provide an indication of what boards need to consider when evaluating their risk appetite. See box, right, for a rundown of its key points. **SR**

KEY QUESTIONS FOR THE BOARDROOM

BACKGROUND

- What are the significant risks the board is willing to take? What are the significant risks the board is not willing to take?
- What are the strategic objectives of the organisation? Are they clear? What is explicit and what is implicit in those objectives?
- Is the board clear about the nature and extent of the significant risks it is willing to take in achieving its strategic objectives?
- Does the board need to establish clearer governance over the risk appetite and tolerance of the organisation?
- What steps has the board taken to ensure the overseeing of risk management?

DESIGNING A RISK APPETITE

- Have the board and management team reviewed the capabilities of the organisation to manage the risks that it faces?
- What are the main features of the organisation's risk culture in terms of tone at the top? Governance? Competency? Decision-making?
- Does an understanding of risk permeate the organisation and its culture?
- Is management incentivised for good risk management?
- How much does the organisation spend on risk management each year? How much does it need to spend?
- How mature is risk management in the organisation? Is the view consistent at different levels of the organisation? Is the answer to these questions based on evidence or speculation?

CONSTRUCTING A RISK APPETITE

- Does the organisation understand clearly why and how it engages with risks?
- Is the organisation addressing all relevant risks or only those that can be captured in risk management processes?
- Does the organisation have a framework for responding to risks?

IMPLEMENTING A RISK APPETITE

- Who are the key external stakeholders and have sufficient soundings been taken of their views? Are those views dealt with appropriately in the final documentation?
- Has the organisation followed a robust approach to developing its risk appetite?
- Did the risk appetite undergo appropriate approval processes, including at the board (or risk oversight committee)?
- Is the risk appetite tailored and proportionate to the organisation?
- What is the evidence that the organisation has implemented the risk appetite effectively?

GOVERNING A RISK APPETITE

- Is the board satisfied with the arrangements for data governance pertaining to risk management data and information?
- Has the board played an active part in the approval, measurement, monitoring and learning from the risk appetite process?
- Does the board have, or does it need, a risk committee to, inter alia, oversee the development and monitoring of the risk appetite framework?

THE JOURNEY IS NOT OVER – FINAL THOUGHTS

- What needs to change for next time round?
- Does the organisation have sufficient and appropriate resources and systems?
- What difference did the process make and how would we like it to have an impact next time round?

Source: Risk Appetite and Tolerance *guidance paper, Institute of Risk Management*

Chain reaction

As production becomes increasingly globalised, businesses need to consider how they would be affected if their suppliers or their suppliers' suppliers fail to deliver

KEY POINTS

01: It is vital to protect your business against disruptions in the supply chain.

02: Factors that could put your suppliers out of action include natural disasters and their wider effects, political volatility, civil unrest, and regulatory and financial problems.

03: Insurance is valuable, but it is equally important to understand your supply chain, and its components and inter-dependencies.

04: Splitting your business between suppliers could reduce risk.

05: Two suppliers located in the same place could be affected by the same issues – so diversify locations.

THE JAPANESE EARTHQUAKE, tsunami and associated power and infrastructure problems were a wake-up call for Western companies about the need to manage supply chain risks. Wherever you source your products and components from, you need to protect your business against disruption of supplies.

Your organisation almost certainly has business interruption insurance – probably linked to a property damage policy – which would protect you in the event of a fire or other disaster. But it is not just an incident at your own premises that can halt your activities. Would your business be able to continue functioning successfully if one of your key suppliers was put out of action?

It is possible to extend your business interruption cover to include disruption from damage to your suppliers' premises. At one time, insurers were prepared to provide this for unspecified suppliers. Now, they are more likely to require details of any suppliers added to your policy. This allows them to identify suppliers in areas where there may be a high risk of natural catastrophes, such as earthquakes and tornadoes, to avoid too much exposure to certain areas.

As it did in Japan earlier this year, a natural disaster can affect vital infrastructure, such as transport links. The ensuing damage to nuclear installations after the earthquake and tsunami necessitated power cuts. Both these factors affected companies outside the immediate earthquake and tsunami damage zone – and led to disruptions in supplies to the West.

It is not only physical damage that could affect your suppliers' ability to deliver. Volatile political situations and civil unrest can also prevent companies from functioning normally and shipping goods out of their country.

In addition, regulatory authorities in the supplier's country may close a plant if it is considered unsafe or fails to meet required standards. There is also the danger that your supplier might experience financial problems or go bust.

For these reasons, some insurers offer contingent business interruption insurance for your supply chain risks, which can be triggered by a wider number of events than just physical damage. A basic rule of thumb is that anything that might stop your business functioning successfully could affect a supplier – with the added risk of a natural catastrophe if the supplier is located in a high-risk area.

Going beyond insurance

Insurance is valuable, but managing your supply chain risk involves more than just buying cover and hoping for the best. The challenges can be particularly great if your business buys goods and components from suppliers in the developing world.

You may have made an initial visit to survey facilities and physical protection measures as well as to agree quality and delivery times, and then incorporated the appropriate provisions into the supply contract. But after that you may have to take quite a lot on trust.

If, for example, a natural catastrophe occurs or the supplier gets into financial difficulties, it may underplay any problems because it does not want to risk losing your business. It is difficult to know what is going on if a supplier is not on your doorstep.

Your risk of disruption is also greater if you minimise the amount of stock you hold, relying on 'just in time'

FEEL THE HEAT: HOW TO PRIORITISE RISKS

Remember that your supply chain risks do not just revolve around business continuity. Suppliers who do not observe your own corporate ethics – for example, if they use underage labour – or meet your quality assurance standards, can affect your reputation.

LIKELIHOOD	insignificant	minor	moderate	major	critical
almost certain	moderate	major	critical	critical	critical
likely	moderate	major	major	critical	critical
possible	moderate	moderate	major	major	critical
unlikely	minor	moderate	moderate	major	critical
rare	minor	minor	moderate	moderate	major

CONSEQUENCE

OUTSOURCING

Outsourcing is increasingly popular among businesses of all sizes, but it introduces new risks:

- Companies relinquish direct control of supply.
- In an increasingly globalised economy, they are relying on an increasing range of far-flung suppliers to cut the cost of the final product and compete in a new global business environment.
- These global suppliers are subject to different risks.
- The increasingly inter-linked nature of suppliers means supply problems have widespread effects.
- Organisations may not have full knowledge of the risks their suppliers face.

Source: Supply Chain Risk Management: A Compilation of Best Practices, *August 2011, Supply Chain Risk Leadership Council*

RISK TIPS

1. Identify your key suppliers – those whose non-delivery would really hurt your business.
2. Assess the likelihood and impact of risks affecting them and their risk management strategies.
3. Prioritise potential vulnerabilities and manage those supplier risks with the highest likelihood and impact.
4. Establish a business continuity plan – and a team to manage it – should a key supplier go down.
5. Where possible, get alternative suppliers on stream.
6. Monitor risks and reassess as necessary.

delivery to meet your contractual obligations to your customers. They may be doing exactly the same, relying on deliveries from you. If this is the case, there will not be a cushion of products for either of you to fall back on, should a vital link in your supply chain break.

Looking into the chain

The first rule for managing your supply chain risk has to be: understand its components and any interdependencies. The longer the supply chain, the more difficult this can be. But even companies producing components and goods in-house cannot be complacent, because they will rely on some raw materials supplied from outside. Moreover, bottlenecks can occur with in-house, as well as external, production.

You need to examine your first tier of suppliers. The questions you should ask are:

1. Are they based in a politically stable country?
2. Does that country have a history of natural catastrophes?
3. Are the suppliers financially robust?
4. Could you replace them quickly and cost effectively if there was a problem?
5. Would you get priority for deliveries if a supplier had a problem that restricted production?

If you are producing goods internally, hopefully only the fourth question will apply. You need to consider whether there is an essential production unit on a site that supplies various parts of your organisation. What happens if there is a major fire?

Question five needs particular thought. Putting aside any assurances that you may have received from the supplier concerned, it will inevitably look after its biggest customer – and that may not be you. It is always worth asking an important supplier who else they deal with, so you can gauge just how much sway you have with them.

Rely on no one

It is also important not to take too much comfort from the existence of other suppliers that you hope can step in if your appointed supplier cannot deliver. The problem could be in your supplier's own supply chain – they could be relying upon a small business, which is also supplying their competitors. If that business goes down, there could be major repercussions for everyone.

As such, if you are sourcing specialist goods or components, it may be worth investigating beyond your tier-one suppliers to find out if they have sources they can call upon if there's a problem.

If you do have a vital supplier in your chain that could cause major problems if it fails to deliver, you need to do some contingency planning. Consider getting other suppliers lined up to fill any gap.

These might also be the first port of call for your competitors if they have problems, so you might have to encourage their loyalty. Splitting your production arrangements between suppliers might minimise your bulk purchase discounts, but could serve you well if one has a problem.

Managing your supply chain risk involves more than just buying cover and hoping for the best. The challenges can be particularly great if you buy goods from suppliers in the developing world

Asking a company that you have not dealt with before to help you out when you have a problem could be difficult if larger competitors are also asking and already have a relationship with them.

Remember, too, that the production of some components tends to be concentrated in particular regions. When the Japan disaster occurred, for example, automotive and electronic companies were the worst hit because the country was an important source of their components. If you have two main suppliers, it would be sensible to ensure that these are not based in the same region, so they would not both be affected by a national natural catastrophe.

If a link in your supply chain fails and if you have to source goods elsewhere at a greater cost, you may be able to recover this additional expenditure. Your business interruption insurance may cover increased cost of working – the money you have to spend to mitigate your total loss. **SR**

Employee safety

Strong health and safety policies and a keen eye on absence levels, both long- and short-term, can reduce both premium costs and the expenses associated with sickness

KEY POINTS

01: A robust health and safety programme saves money in insurance premiums and on staff turnover and retraining.

02: Absence management aims to find the line between supporting employees with health problems and preventing employees taking advantage of sick pay schemes.

03: Short-term and long-term absenteeism can be dealt with by restricting sick pay, return-to-work interviews and involving trained line managers in reviewing attendance.

A demonstrable, robust health and safety risk management system has benefits beyond protecting employees. It also helps ensure that your employers' liability premium is competitive, as well as reducing uninsured costs such as lost time, staff turnover and retraining. The Health and Safety Executive estimates that for every £1 recovered through insurance, the total unrecovered loss exceeds £11.

Of course, you have to meet the safety management requirements laid down by legislation such as the Health and Safety at Work Act, the Management of Health and Safety at Work Regulations and any regulations specific to your industry sector. But that is just the minimum expected of every company.

As well as protecting employees' safety with your health and safety programme, you might also consider absence management. The cost benefits can be considerable and should far outweigh your investment.

According to the Chartered Institute of Personnel and Development (CIPD), effective absence management involves finding a balance between helping employees with health problems stay in – and return to – work, and taking consistent and firm action against employees who try to take advantage of occupational sick pay schemes.

Measuring and managing absence

A key element in managing absence effectively is accurate measurement and monitoring. Measures can be used as trigger points, indicating when you need to investigate absence. Monitoring absence allows you to identify trends and to explore underlying causes.

In the latest CIPD absence survey, fewer than half of employers say they monitor the cost of absence, just under half of organisations have set a target for reducing absence, and just over one-third benchmark themselves against other employers.

According to the CIPD, effective interventions in managing both short-term and long-term absence include restricting sick pay and enforcing return-to-work interviews.

In addition, using trigger mechanisms to review attendance, involving trained line managers to manage and review attendance, bringing in occupational health professionals, and disciplinary procedures for unacceptable absence levels can be used to deal with short-term absence.

Long-term absence can be tackled using occupational health involvement and proactive measures to support staff health and wellbeing, changes to work patterns or environment and introducing rehabilitation programmes. **SR**

A FRAMEWORK FOR CONTINUOUS IMPROVEMENT

- Have an effective written policy that details the organisation and arrangements for health and safety; as well as reflecting what actually happens and detailing health and safety objectives.
- Plan to achieve health and safety objectives by having: effective management control; clear allocation of responsibilities and resources; good communication; competent individuals; and employee consultation.
- Plan based on risk assessments and prioritising actions to eliminate or implement safe work methods to control significant risks.
- Measure health and safety performance by proactive inspections and undertaking reactive accident/incident investigation.
- Review health and safety arrangements and implement any necessary improvements to your company's health and safety management system.
- Have an audit, preferably independent, that compares your health and safety risk management system with your competitors' and best practice.

Source: Department for Business, Innovation and Skills (formerly Department of Trade & Industry)

RISK TIPS

1. Identify hazards in your workplace.
2. Assess the risks from these hazards.
3. Introduce safe working procedures for employees to follow.
4. Train your employees in the risks and necessary controls.
5. Monitor the work to ensure it is being done safely and the workplace to ensure it is always safe to work in.
6. Record:
   - risk assessments you have carried out for the working environment and specific high-risk activities;
   - safe working procedures for activities deemed to be high risk;
   - training that is given, to follow safe working procedures;
   - workplace inspections, to ensure that safe working procedures are being followed; and
   - incidents and investigations, to ensure similar problems do not happen again.

Source: Department for Business, Innovation and Skills

Recalls and reputation

As more businesses are being hit by product recalls, insurers have made cover easier and cheaper – even providing short-term specialist consultants for smaller companies that don't have a large public relations budget

MANY COMPANIES INSURE AGAINST the risk of their products being defective but fail to consider recall insurance, despite the considerable financial and reputational costs of recalls.

With tighter legal requirements, more European companies than ever are notifying the authorities of potentially dangerous products. Inevitably, the number of product recalls required is increasing.

Don't underestimate the potential costs of a recall. These can include:

- tracing where the affected products might be, for example, in your warehouses, in your customers' warehouses, on the shelves or with the end customer;
- the cost of getting products back;
- advertising expenses;
- testing product samples and possibly external laboratory fees;
- repairing products where appropriate, or disposing of products where not;
- business interruption while production sites are closed for investigation;
- possible loss of business from disaffected customers; and
- management time spent on dealing with the crisis.

Avoiding the likelihood of a recall is particularly difficult for mid-sized companies. The business may not have a lot of resources to invest in risk management and quality assurance. At the same time, in a bid to reduce costs, it may well be outsourcing goods or components from companies in developing countries whose standards are lower than those that would be applied to in-house production.

China is the single greatest source of notified potentially dangerous products. According to law firm Reynolds Porter Chamberlain, UK recalls of goods made in China represented as much as 62% of all consumer recalls last year.

The firm says that the comparatively low production standards of some Chinese goods entering the UK market is a major trigger of health and safety alerts. Partner Stuart White adds: "This is a major issue for UK or European companies, as they are increasingly dependent on production in China. A higher percentage of consumer goods from China means more companies will have to undertake expensive recalls."

Specialists can help

While you will have insured product liability – the risk that your product may cause third-party property damage or injury – you may not have considered recall insurance.

At one time, recall insurance was both comparatively expensive and not widely available. Now, product recalls have become more common and businesses more aware of the need to protect themselves. And a wider spread of risk, with more insurers prepared to provide this cover, has brought premiums down. Some insurers also cover the cost of specialist consultants to help companies avoid long-term reputation damage.

A product recall is one of the few situations where you have to publicise your company's shortcoming. But you should institute the recall as quickly as possible. Delaying could result in customer claims, increase costs and reputational damage. Yet, however quickly you act, you must be prepared for some brand damage and a possible drop in market share, which is where specialist consultants come in.

Be prepared to close a production line while you investigate the causes of the recall. If you have planned well for business interruption, this may not be a problem, as you may have another facility to switch to. If you don't have an alternative immediately available, you won't be able to meet ongoing delivery commitments and you're likely to lose business as a result. **SR**

KEY POINTS

01: The potential costs of a recall are considerable and the number of recalls is increasing, but many businesses continue to see recall insurance as a luxury.

02: Medium-sized companies may be vulnerable if they cannot invest enough in quality assurance.

03: Recall cover, often including specialist consultants to help reputation management, is becoming cheaper.

RISK TIPS

1. Don't stint on investing in quality management and product safety. Your company is only as good as your products so it's money well spent
2. Monitor customer complaints as these can serve as an early warning system of a defective product
3. Producing goods in smaller batches can reduce costs if you need to recall a defective batch
4. Make sure that contracts specify that your suppliers are responsible for the costs of any recall that involves their defective products or components
5. Establish a crisis management plan and appoint a recall management team before rather than after any recall
6. Insure your recall risk with a policy that covers the cost of expert consultants to minimise reputational damage
7. Act quickly if you do need to make a recall to minimise the likelihood of potential claims from customers and reputational damage.

Handling cyber risk

Cyber crime is becoming an increasingly prevalent and costly risk, yet many businesses are woefully underprepared for an attack – a major business failing in this digital age

KEY POINTS

01: Businesses are at threat of cyber crime regardless of their size.

02: Traditional property and liability insurance policies will not give protection against risks like data breaches.

03: Reputational damage from cyber crime can be irreparable.

04: Attacks can come from within a company, as well external parties.

05: Confidential information can be leaked through staff chatting on social networking sites.

COMPANIES OF ALL SIZES TODAY ARE dependent on IT to a greater or lesser extent. Large multinational corporations have the resources to plough considerable investment into ensuring that their IT security is robust and updated regularly to take account of any changes in the risk environment. However, even they can get it wrong, as demonstrated by recent data breaches occurring at Epsilon, Sony and Citigroup.

Mid-sized companies, although lacking the resources to make a similar investment, may consider that their size makes them a less attractive target for hackers. XL senior underwriter, professional lines, Dawn Simmons says this is a fallacy. "Recent reports suggest that hackers are more likely to target smaller rather than larger companies because they consider it will be easier to hack into their systems."

Simmons warns: "The combination of more sophisticated criminals and stricter data breach laws results in companies facing increasing financial and reputational exposures. The average cost of a data breach in Europe in 2010 was approximately £1.9m, and we expect that number to rise in the future.

"In the light of stricter laws being implemented throughout Europe, companies from all sectors need to protect themselves against the soaring costs associated with hacker attacks, lost data or human error."

Specific policies

Traditional property and liability insurance policies do not give your company protection against specific risks such as data breaches and associated costs arising in today's hi-tech business world. Crime policies also do not fill the gap, as they generally focus on loss of money and securities. But if your company suffers a data breach, it can expect to pay the often considerable costs associated with issuing mandatory data breach notifications to customers and authorities, as well as civil regulatory fines and penalties.

For this reason, some insurers have introduced specific cyber risk policies. In addition to fines, penalties and notification costs, these may also cover other expenses.

For example, XL's Eclipse policy also offers companies cover for IT forensics – the cost of hiring a specialist IT security firm to investigate how a data breach has happened and what to do to prevent a recurrence. It can also compensate for possible business interruption resulting from a breach, as well as the costs of public relations specialists to manage reputational fall-out.

"The reputational damage resulting from a data breach can be horrendous," Simmons says. "The loss to the business can be as much as £5m [€5.74m] or even £10m."

While a loss of this size may not have a negative impact on the balance sheets to large multinationals, the effect for smaller businesses may be devastating. "Reputation risk can ruin a smaller company," Simmons warns.

Insurance is one of the tools that mid-sized companies can use to protect themselves. But you also need to consider

GROWING COST OF DATA BREACHES

SYMANTEC CORP AND THE PONEMON Institute reported that the average cost of a data breach in the UK in 2010 was £1.9m (€2.18m) or £71 per record, an increase of 13% on 2009, and 18% on 2008.

The incident size ranged from 6,900 to 72,000 records, with the cost of each breach varying from £36,000 to £6.2m. The most expensive incident increased by £2.3m compared with 2009.

The report said that hostile attacks reign as the most expensive data breach for UK organisations. Malicious or criminal attacks accounted for 29% of all data breaches. "The expenses associated with a data breach range from detection, escalation, notification, and customer churn due to diminished trust," said the study.

Lost business ranked as the biggest contributor to overall data breach costs. Recovering customers, profits and business opportunities after data breaches posed the greatest cost hurdles for companies in 2010. Lost business accounted for 48% of the total.

Other contributing factors were costs sustained in the immediate aftermath of the event, such as resetting accounts and communicating with customers (known as ex-post response) at 23%, and costs related to detection/escalation at 20%.

your cyber risk management strategies. Having robust controls will make your business a more appealing risk for insurers, ensuring not only that you will be offered cover but also that you are quoted a competitive premium. Reports suggest that the most common causes of data breaches are website hackers and stolen hardware such as laptops, so these are the areas to focus on.

It isn't only data breaches that cause problems. Erasure of data also remains an ongoing risk, whether accidentally or knowingly perpetrated – usually by disaffected employees.

Key risk management strategies here include backing up vital information and storing the back-up in a location outside of your premises in case of fire or other damage.

As far as malicious erasure is concerned, it is important to make sure that the passwords of any employees who leave are cancelled, so that they cannot access your system afterwards.

Leakage of confidential information

One risk that some of the major multinationals are grappling with today is potential leakage of confidential or potentially reputation damaging information through employees 'chatting' on social networks.

According to research published in September by global risk consultancy Protiviti, around one in six (17%) of UK employees consider social networking such as Facebook and LinkedIn a major risk to corporate security – and even more (27%) feel that employers should provide clearer guidelines on using social media in the workplace. **SR**

CLOUD COMPUTING/HOSTED SYSTEMS SECURITY

IF YOU PUT YOUR NETWORK INTO THE cloud or use hosted systems, then you are making someone else responsible for your security and need to ask your supplier a number of questions. These could (and indeed should) include:

- What security and authentication procedures are in place for remote staff access?
- How is data secured against leakage?
- What protection is there against DDoS attacks?
- How can you guarantee your staff won't access my company's data?
- What is the service level agreement for availability and what is the recourse if it is breached?
- In what jurisdiction is my data held and stored?

Source: Ian Kilpatrick, chairman of IT specialist Wick Hill Group

ADVICE FROM THE INFORMATION COMMISSIONER

COMPANIES LOOKING FOR COMPLETE computer security should:

- Install a firewall and virus-checking software on your computers.
- Make sure that your operating system is set up to receive automatic updates.
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
- Only allow your staff access to the information they need to do their job and don't let them share passwords.
- Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Take regular back-ups and keep them in a separate place so that, if you lose your computers, you don't lose the information.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- Consider installing an anti-spyware tool.

RISK TIPS

1. Be prepared to invest adequately in IT security.
2. Make employees aware of your data privacy policy and restrict access to confidential information on a need-to-know basis.
3. Protect your business against disruption with a continuity plan – and test it regularly to make sure it still works.
4. Make sure that any data loaded onto employees' laptops and other mobile devices is encrypted.
5. If you are outsourcing your IT security to a third-party vendor, check that this vendor is financially solvent and has appropriate security and cyber coverage, and make sure that your contract makes the vendor responsible for protecting your data.
6. Provide social media guidelines for employees with information on what they can and cannot say.
7. Classify information in-house to clearly indicate whether it is restricted for internal use only or can be made public.

A legal minefield

Ethical standards for businesses are about to get stricter, so senior managers and directors will need to take a far more hands-on role in ensuring that their firms comply with the rules

KEY POINTS

01: The Corporate Manslaughter Act does not impose new duties, but it is an added incentive for firms to take their health and safety obligations seriously, as juries will consider this.

02: The Bribery Act lists six core principles designed to ensure that businesses compete fairly at home and abroad.

03: The government has listed the categories to be aware of when ensuring there is no discrimination against existing or potential employees.

WHERE THERE'S A LAW, THERE'S A liability. And getting caught out by regulations can be expensive. There are myriad rules and regulations beyond the Companies Act that govern corporate behaviour. Some impose a liability not just on the company, but on individual directors and senior managers found to have been negligent. Several of these laws are covered in this guide. But it is also important to be aware of some relatively recent additional legislation.

Corporate manslaughter

The offence of corporate manslaughter (known as corporate homicide in Scotland) came into force in April 2008. Unlike the original proposals, the Corporate Manslaughter Act does not impose new duties or obligations, but it is an added incentive for companies to take their health and safety obligations seriously.

Health and Safety Executive guidelines state that juries are required to consider breaches of health and safety legislation in determining the liability of companies and other corporate bodies for corporate manslaughter/homicide. "Juries may also consider whether a company or organisation has taken account of any appropriate health and safety guidance and the extent to which the evidence shows that there were attitudes, policies, systems or accepted practices within the organisation that were likely to have encouraged any serious management failure or have produced tolerance of it," says the guidance.

Penalties for corporate manslaughter include unlimited fines, remedial orders and publicity orders. A remedial order will require a company or organisation to take steps to remedy any management failure that led to a death. The court can also impose an order requiring the company or organisation to publicise that it has been convicted of the offence, giving the details, any fine imposed and the terms of any remedial order made.

Facilitation payments were already banned, but perhaps transgressions were not too hotly pursued, as even mega UK companies seem to be taken aback by this provision

The original idea behind the legislation was to make it easier to pursue large corporations – and individuals within them – in connection with incidents involving fatalities. It was initiated in response to events such as the 1987 Zeebrugge ferry disaster. But after a slow consultancy process, the provisions were watered down. As it stands, individuals cannot be prosecuted under the act, although they can be prosecuted for existing health and safety offences and gross negligence manslaughter.

No prosecution of a large company has yet occurred. The only case to date involved the small business of Cotswold Geotechnical Holdings. But it is definitely something for mid-sized companies to watch out for. A proactive approach to health and safety management could mean the difference between a successful or unsuccessful defence.

Bribery and corruption

Oiling the wheels of business is a time-honoured strategy. But where do you draw the line? The Bribery Act, which came into force in July 2011, sets the bar.

The act focuses on six core principles (see box, opposite) designed to ensure businesses compete fairly and ethically – on home turf and overseas. Individuals found guilty of a bribery offence can be fined, spend up to 10 years in prison or both. There is no limit on fines for corporate organisations. There will also be collateral consequences of a conviction, director disqualification, debarment from public procurement and asset confiscation.

The good news is that reasonable hospitality to cement business relationships

RISK TIPS: BRIBERY AND CORRUPTION

1. The board of directors will have overall responsibility for designing and implementing an anti-corruption programme and establishing an anti-corruption culture.
2. A senior officer will be directly accountable for the implementation and running of the programme.
3. Organisations must incorporate anti-corruption elements into their code of conduct, risk management, due diligence, decision-making, procurement and contract management, employee-vetting and disciplinary procedures. The organisation must ensure that relevant members of staff are appropriately trained in these areas.
4. Organisations should establish gifts and hospitality policies and registers.
5. Companies must establish whistle-blowing procedures and properly investigate all allegations.

Source: Ministry of Justice, Adequate Procedures Guidance

RISK TIPS: CORPORATE MANSLAUGHER

1. Ensure that the board reviews health and safety performance at least once a year.
2. Examine whether your health and safety policy reflects your company's current priorities, plans and targets.
3. Check the effectiveness of risk management and other health and safety systems reporting to the board.
4. Report any health and safety shortcomings and the effect of relevant board and management decisions.
5. Decide actions to address any weaknesses and a system to monitor their implementation.
6. Consider immediate reviews in the light of major shortcomings or events.

Source: Leading Health and Safety at Work – *Institute of Directors and the Health and Safety Commission*

is fine. The bad news is that facilitation payments are banned. They were already, but perhaps transgressions were not too hotly pursued, as even mega UK companies seem to be taken aback by this provision. This means the law is even more prescriptive than the US Foreign Corrupt Practices Act.

Anti-discrimination legislation

There is a huge amount of legislation designed to prevent companies discriminating against employees or potential recruits. The UK government's online information service, Directgov, lists the categories to be aware of:

- gender;
- marriage or civil partnership;
- gender reassignment;
- pregnancy and maternity leave;
- sexual orientation;
- disability;
- race;
- colour;
- ethnic background;
- nationality;
- religion or belief; and
- age.

In addition, you can't dismiss or treat less favourably employees who work part time or are on fixed-term contracts.

For mid-sized companies, this can be a difficult area. With a smaller employee base than their large counterparts, they want to ensure that new employees fit in and may try to take the perceived prejudices of existing employees into account. But this could be an expensive mistake.

The risk here is a matter of common sense. Treating all employees equally and wording recruitment advertising so that it does not exclude any people within the listed categories should be standard practice.

Navigating the minefield

Directors' and officers' liability insurance is designed to protect a firm's senior management against allegations of wrongful acts. With so much legislation stacked against these individuals, one would suppose that actions could come from all directions. That may be the case for large multinationals, but the reality for mid-sized companies in the UK is different.

XL's head of international professional lines in continental Europe, Beatrice Salter, points out that companies of this size tend to be protected against the main source of claims for large multinationals – shareholder actions. "Generally, these companies do not have a similar large number of powerful shareholders, so actions by such investors are comparatively rare," she says.

Salter believes that most actions are related to company failure – bankruptcy and insolvency. While being the director of a company that fails is not a crime, wrongful trading – that is, continuing to do business when you believe your company is insolvent or after a liquidator or receiver has been appointed – most certainly is.

While mid-sized companies may not have a large number of powerful activist shareholders, they do have employees – and Salter says these are the second-largest source of claims. "There is potential for employment practice liability-related claims within this sector," she warns.

Knowing the UK anti-discrimination laws is important – but these are a mere "pussy cat" compared with US rules, she says. North America has very stringent regulations on employment practices, privacy and discrimination so if you have a representative office in the USA, make sure that you observe these rules or you will leave yourself vulnerable to very expensive action, Salter adds.

Even in Europe, cultures differ. For example, in Germany, female employees may not be over-enamoured by the kiss-on-cheek greetings prevalent in other parts of Europe. It's a matter of understanding where you are doing business and how your employees expect to be treated. **SR**

ANTI-BRIBERY PRINCIPLES

PROPORTIONATE PROCEDURES

The actions you take should be proportionate to the risks you face and to the size of your business.

TOP-LEVEL COMMITMENT

The board is expected to lead on issues such as a zero tolerance culture, an anti-bribery code of conduct, risk assessment and general breaches of procedure.

RISK ASSESSMENT

The company needs to assess external bribery risks – such as country, sector, transaction, opportunity and business relationship risk – and put in place procedures to mitigate such risks.

DUE DILIGENCE

The organisation needs to know exactly who it is dealing with, particularly those who are conducting business on its behalf, as it is responsible for such third parties and agents.

COMMUNICATION (INCLUDING TRAINING)

It is vital to communicate your policies and procedures to staff and other associated organisations and people, and this should be backed-up with effective scenario-based training – whether web-based or face-to-face.

MONITORING AND REVIEW

The company needs to update its procedures over time and test whether they are operating effectively. External reviews may be helpful.

Source: BDO LLP

Preventing pollution

As green concerns steadily grow in the public's consciousness, so too does the rigidity of enviornmental liability regulations for businesses throughout Europe

KEY POINTS

01: Businesses can face enormous costs for environmental failings, regardless of the company's size.

02: Association with an environmental crisis or disaster has increasing reputational consequences, as the public becomes more aware of green issues.

03: A public liability policy will not cover fines relating to environmental liabilities.

IN THE LAST 20 YEARS, ENVIRONMENTAL liability has risen rapidly up the corporate risk agenda. It isn't just the large multinationals that are exposed to unlimited fines, heavy clean-up costs and potential compensation payments. Mid-sized businesses too should consider the need to manage this risk.

With incidents like the BP oil spill hitting the headlines and reports of multibillion-pound compensation claims, you might be forgiven for thinking that pollution is primarily a problem for the 'big boys'. But there are plenty of incidents that may not make the national press of smaller companies falling foul of environmental regulations. And the increased amount of environmental regulation that has taken place in recent years makes it much more likely that you could experience a claim.

For many years, all companies have faced liability for 'nuisance' under civil law. But the regime became much tougher with the introduction of EU directives, now incorporated in UK law in the Environmental Protection Act, as well as more recent supplementary regulations introduced two years ago. In addition, there are specific rules relating to perceived high-risk businesses.

Without going into the legislation in detail, the key points to remember are:

- The polluter pays. If your business has caused the damage, you are responsible for the costs of remedying it, with very few exceptions.
- If there is a risk of environmental damage from your business activities you must prevent this damage (or further damage if the problem already exists) from occurring.
- Tell the appropriate authority (the Environment Agency, in England) of any risk or damage and follow instructions on prevention and/or remediation.
- Directors may be held personally liable for offences caused with their consent, connivance or neglect.

The implications of causing environmental damage are not just financial. An incident can also damage your reputation, affecting customers' view of your business and their willingness to deal with you. Some large companies will scrutinise your environmental management policy before doing business with you.

Transferring the risk

There is a common mistaken belief that a public liability insurance policy will cover environmental risks. Unfortunately, this is far from the case. Your public liability insurance provides compensation for your legal liability for third-party property damage or bodily injury. It will also contain an exclusion relating to gradual pollution and restricting cover to sudden accidental and unexpected incidents only.

Even if you have an unexpected incident, your public liability policy will not cover you for any fines relating to environmental liabilities. It won't pay for remediation costs where you're required to clean up contamination, as no third-party compensation is involved. Similarly, if you voluntarily agree to pay for clean-up costs, in the absence of legal liability your public liability policy won't indemnify you.

Some insurers have stepped in, with environmental impairment liability policies offering a range of covers. Environmental impairment liability insurance can cover both on- and off-site risks. It can include: third-party liability; on-site clean-up costs; off-site clean-up costs; the costs of business interruption should you need to close a site during clean-up; and third-party business interruption costs, as well as legal defence costs. In addition, any day-to-day exposure aside, if you are embarking on a construction project or a transaction such as a merger or acquisition, you need to take any actual or potential environmental liability exposures into account.

If you're buying a site that has been contaminated but is now cleaned up to current standards, don't be complacent. Rigorous legislative requirements may mean that further work is needed. If the seller is out of the picture, you may end up with the cost.

Similarly, if you're merging, acquiring or even divesting, there may be environmental issues relating to the business concerned. Appropriate insurance can oil the wheels of the deal by providing cover should any business providing warranties or indemnities not be around in a few years' time. **SR**

RISK TIPS

1. If there's a possibility of pollution arising out of your business activities, implement an environmental management system.
2. Assess sites at the start and end of your operations there so that any pollution can be detected and remediated.
3. Identify operations and processes that could pose environmental problems.
4. Evaluate systems and procedures available to manage these issues.
5. Comply with any health and safety rules on handling toxic or contaminating substances.
6. Tell your stakeholders how you deal with environmental matters.
7. Tell your insurer immediately if you discover any incident involving pollution as prompt action will reduce any damage.

Considering claims

From taking out a policy to making a claim, in the insurance world your business depends on honesty and accuracy. Anything else could result in serious financial straits

IT IS A FORTUNATE COMPANY THAT never experiences any claims, so it's important to know how to maximise your chances of recovering in full if you have a claim against your insurer, and how to minimise the likelihood of a successful claim against you. Key areas are full disclosure when you take out your insurance, accurately estimating what a loss might cost you, and defensibility.

If you have an insured claim, you or your broker must let your insurer know within the time limit specified in your policy. In the case of property damage, you need to substantiate the amount of the loss. If the claim is large, it's likely that your insurer will appoint a loss adjuster to investigate the loss and negotiate settlement.

When you complete an insurance proposal or provide information to your brokers so that they can place your risk in the insurance market, you must give full details of any material facts. These are facts that you know (or ought to know) that could affect the way that insurers view your risks and the amount of premium they charge.

If you leave out any material facts, your insurer has the right to void cover. Material facts might include a poor claims history, any claims that you know or believe are pending, or misrepresenting the physical securities that you have in place to protect your property. The sensible rule here has to be: if in doubt, disclose it.

The importance of accuracy

When you are insuring property, you need to consider values very carefully. If you're insuring on an indemnity basis, the insurer will pay compensation based on the value of your property at the time of any loss. You will only be entitled to an amount equivalent to what it would cost to buy or rebuild that property in its current condition.

For example, if you are insuring your computer equipment on an indemnity basis, you will receive a sum that allows you to buy the same equipment second-hand, with no allowance for upgrading.

Most companies that have a significant loss will want to take the opportunity to upgrade their premises or property. In this case, you should consider insuring on a 'reinstatement as new' basis.

Whatever basis of compensation you select, you must make sure that the valuation (sum insured) that you decide upon accurately reflects the amount you will need. This is essential because, if you have undervalued the cost of replacement or reinstatement as new, your insurer is entitled to reduce the compensation it pays by the same proportion.

This 'average' clause is one of the main reasons companies that consider themselves adequately insured can find themselves in financial straits after a loss. Remember, when selecting a replacement sum insured, it's important to include the 'extras' associated with a total loss. These can incorporate things like the cost of complying with public authority requirements, disaster recovery, debris removal and professional fees. Otherwise, with the total loss exceeding the sum insured, average will apply.

The amount you insure for business interruption and the time you estimate it will take your business to get back on its feet again also need to be accurate. It's important here to take account of not only the effects of damage to your own premises but also the consequences of a key supplier being out of action for some time.

A business interruption review that includes looking at the supply chain will help you to assess the amount and type of coverage you need.

Demonstrating defensibility

If someone makes a claim against your company – whether insured or uninsured – you need to be able to put up a robust defence. A key part of good risk management has to be building defensibility into your systems and processes.

If you can demonstrate good working practices and a history of care in safeguarding employees, members of the public and customers, this will go a long way in protecting you against successful liability claims.

This is particularly important in refuting spurious or exaggerated claims and documenting incidents is key here. You should record, report and investigate any incidents that could lead to a claim. SR

KEY POINTS

01: It's vital to be prompt and honest in your disclosures and claims, lest your insurer void cover.

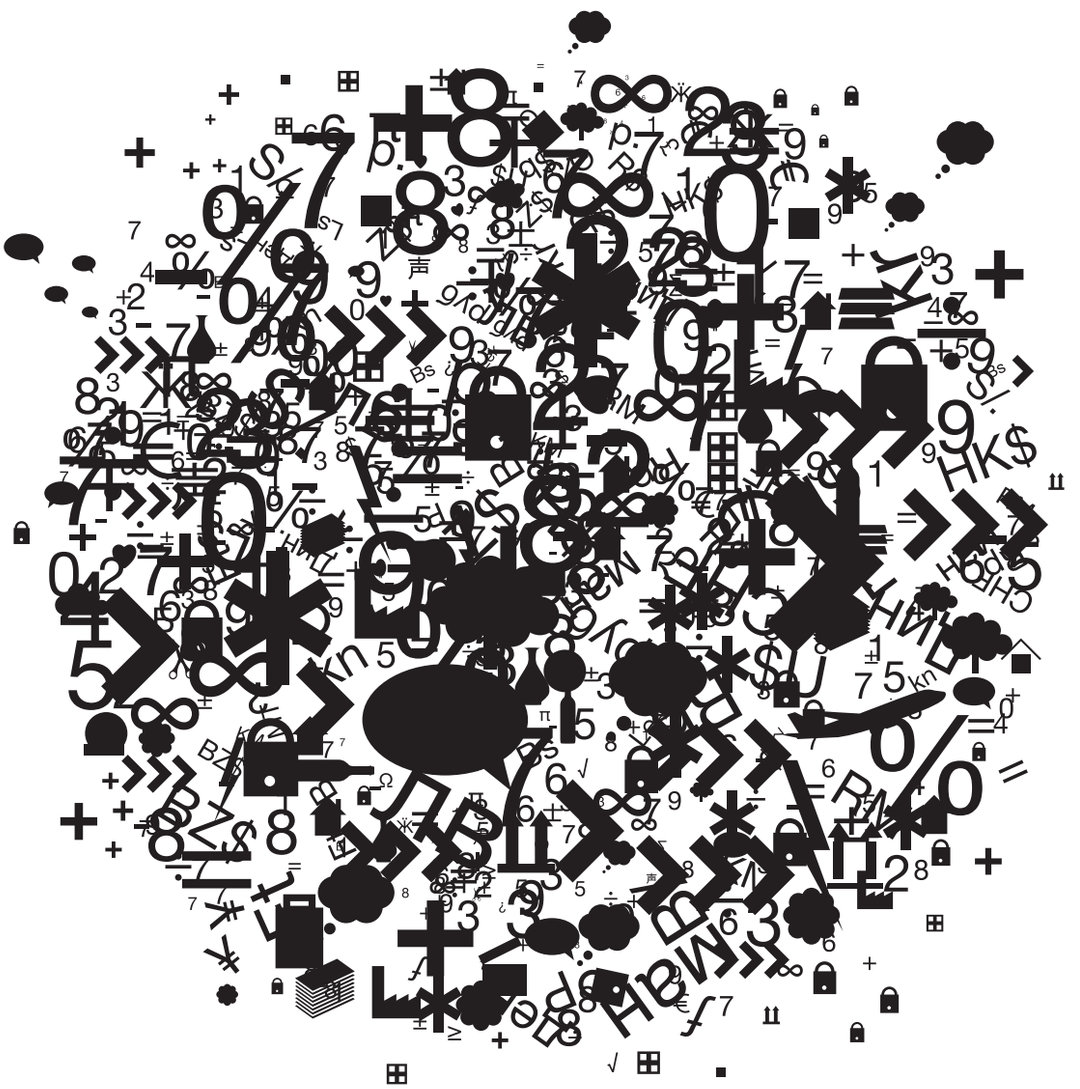
02: Give special consideration to values – insuring technical equipment on a replacement basis will not make allowances for upgrades, for example.

03: Good working practices and corporate responsibility can help safeguard against successful liability claims.

RISK TIPS

1. Make full disclosure of any facts that could affect how insurers view your business.
2. Make sure your property valuations are accurate to avoid insurers scaling down compensation.
3. Consider a business interruption review that takes account of suppliers' disruption as well as your own to ensure sums insured and period of indemnity accurately reflect your risk.
4. Notify insured claims within the time specified by the underwriter.
5. Substantiate the amount of any property loss.
6. Maximise your chances of defending liability claims successfully by demonstrably robust risk management and full documentation of incidents.

XL Group
Insurance
Reinsurance



Properties, transport, energy, art, manufacturing, insurance, aerospace, contracts or people.
Whatever your world is made of, we're here to help your business move forward.

MAKE YOUR WORLD GO

xlgroup.com