Managing Risk

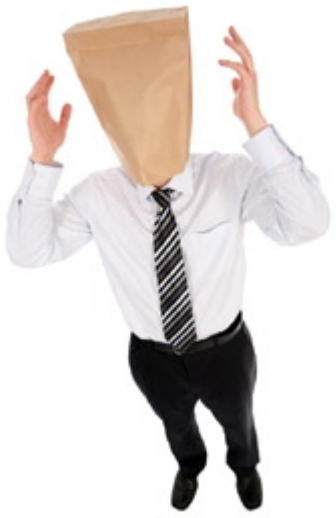
The Encore Risk Management Group Inc

More than a Policy — A Partnership!

Media Plus Insurance Services

Post Office Box 36219 Birmingham, AL 35236
Toll Free: 888.204.4364 or Fax: 205.444.3035
www.mediaplusins.com

Risk Management | Winter 2009 | Volume 19 • Number 1



Reputation: The Sum of All Risks

When Bear Stearns collapsed in March many financial columnists gave many explanations for the demise of the fifth-largest investment bank in the country. But the simple truth was that investors lost confidence in the bank's ability to repay its loans. In other words, the giant financial institution collapsed because it failed to manage its reputation.

No surprise then that a 2006 report by the respected Economist Intelligence Unit noted that "protecting a firm's reputation is the most important and difficult task facing senior risk managers." In a survey, 84 percent of senior risk managers felt that risks to their company's reputation had increased significantly over the previous five years due to the development of global media and communication channels, increased scrutiny from regulators and reduced customer loyalty. Reputation risk now ranks as a greater concern than regulatory risk, human capital risk, IT network risk, market risk and credit risk, the survey found. That's because reputation risk is the risk of risks — it can arise when any other risk is not controlled, causing customers, investors and analysts to downgrade their view of the company and its products or services.

Risk managers who try to manage this threat primarily through insurance would probably soon find themselves looking for a new line of work. Some policies reimburse companies for crisis management costs, while others help them deal with frequent causes of reputation failure such as product liability and recall insurance and errors and omissions coverage. Examples include AIG's Crisis Containment policy, which offers reimbursement of fees and costs of expert consultants responding to one of 17 specified crises. Another is brand protection insurance from Swiss Re. Many product liability and recall policies also include endorsements for crisis management costs. However, no insurance policy can restore a corporation's stock to its pre-loss levels.

The best approach to minimize reputation risk exposures is to analyze the potential risk and identify actions to manage that risk — which may or may not include buying insurance coverages. The input of others will be invaluable in this task.

For example, the company's legal department or legal counsel — how do they see risk? What risk factors does the company include in public disclosures? What are other potential sources of reputation risk? The company's insurance broker can provide possible solutions to some of the specific risks identified.

The final stage involves the drafting of contingency plans to deal with specific situations. A PR

REPUTATION—continued on Page 3

Risk Note

Employers' first aid requirements differ from sector to sector and from workplace to workplace. You can use the OSHA 300 log, OSHA 301 forms and your workers' compensation carrier's reports to help identify first aid needs. The Bureau of Labor Statistics can also provide insight into the risks particular to your industry (www.bls.gov/iif).

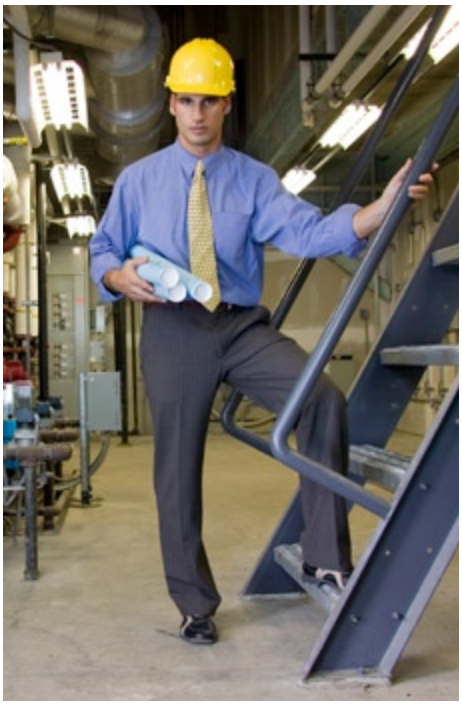
To set up your program, you can use the guidelines in OSHA's "Best Practices Guide: Fundamentals of a Workplace First-Aid Program," at www.osha.gov/Publications/OSHA3317first-aid.pdf.

The guide details the four primary components of a workplace first-aid program:

- **Identifying and assessing workplace risks**
- **Designing a program that is specific to the worksite and that complies with OSHA requirements**
- **Developing written policies and teaching workers about the program**
- **Evaluating and modifying the program to keep it current, including regular assessment of the first-aid training course.**

Contractor or Employee? That Is The Question

Hiring someone as an independent contractor can save businesses significant sums by eliminating workers' compensation insurance, employee benefits and payroll taxes. But complex rules determine whether someone is an employee or a contractor. Getting them wrong can have serious consequences – back taxes, penalties, fines, lawsuits and damage to morale, to name just a few.



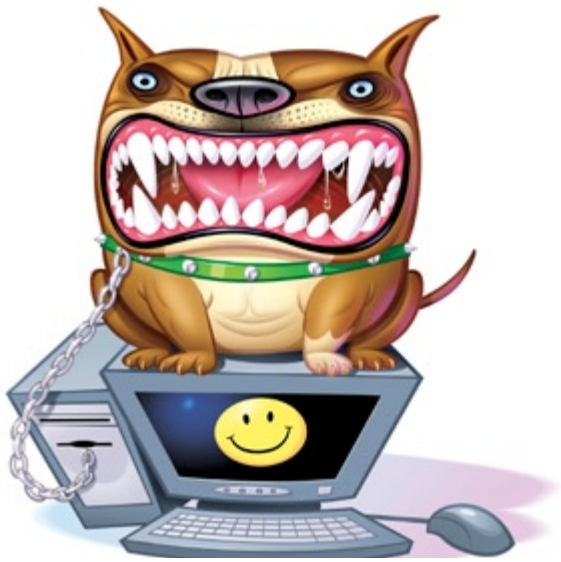
Discerning the difference between an independent contractor and employee can be a complex and imprecise art, especially when telecommuting blurs the use of location as an indicator of employment status. The IRS has a comprehensive list of factors that it uses to determine a worker's status. Many states have additional requirements, which are supplemented by numerous legal rulings.

Generally speaking, the more independence workers have, the more likely they can be classified as independent contractors. Therefore, employers should also look at whether the worker advertises his services to others, employs assistants or purchases his own workers' comp insurance. You can also fill out an IRS form SS-8 to determine worker status.

Employee	Not
Worker must obey instructions concerning when or how to perform the job.	Worker responsible for the outcome of the job and can determine how it is to be done.
Company provides training.	Worker may be licensed by a state board; may have invested considerable sums in training.
The job is "integrated," or central to the company's operations — the more integrated, the more likely the worker will be considered an employee.	The job is not necessarily integrated to the company's operations.
Services must be performed by a particular person.	Work can be performed by anyone.
The company hires, supervises or pays a worker's assistants.	Worker can hire assistants and is responsible for their pay.
Worker has an ongoing relationship with the company.	Worker advertises or otherwise makes his/her services available to the general public.
Company sets the work hours.	Worker can set his/her own work hours.
Company requires full time work at its business.	Worker can work for more than one company at the same time.
Company controls where the work is performed.	Worker determines where the work is performed.
Company determines the order in which tasks are to be done.	Worker controls task order.
Company requires oral or written reports.	
Worker receives payment by hour, week or month.	Independent contractors are usually paid on a per job or commission basis.
Company provides tools and materials.	Worker has made a significant investment in tools or facilities.
Company pays travel/ business expenses.	Worker can realize a profit or loss from a job.
Company can discharge a worker for reasons other than not meeting a contract's terms.	Worker has a contract with the company.
Worker can usually quit without liability for failure to complete a job.	Worker liable for completing a job according to contract.

Controlling Cyber Risk and Your Budget

The most recent survey by the Computer Security Institute found that only 29 percent of companies purchased cyber-risk insurance policies. The low numbers reflect misunderstanding of the risks involved, overly complex offerings from many insurers and premiums that can seem prohibitive. Knowledgeable brokers can help insurance buyers navigate this important area of risk management, say experts.



Practically every company that uses a computer faces cyber risks of one sort or another. But cyber insurance is designed to do far more than just indemnify a company for damage done to its computer systems.

Policies are nonstandard and vary from insurer to insurer. They can provide business interruption insurance if the data losses cause a company to suspend operations. They can cover liability-related costs such as defense costs, settlements, judgments and sometimes punitive damages incurred by a company stemming from its computer systems or online presence. These include breach of privacy due to theft of data (such as credit card, financial or health-related data); transmission of a computer virus or other problems resulting from a computer attack that cause financial loss to third parties; a security failure that causes network systems to be unavailable to third parties; and allegations of copyright or trademark infringement, libel, slander, defamation or other "media" activities on the company's Web site, or by company employees.

In addition, many policies provide insureds access to an identity theft call center that will assist customers or employees if their personal information is stolen from your systems. Some policies even offer cyber-extortion endorsements that cover the "settlement" of an extortion threat against a company's network, as well as the cost of hiring a security firm to track down and negotiate with blackmailers.

So why are so many companies overlooking the dangers posed by cyber risk and the solutions offered by well-tailored insurance policies?

Mark Greisiger, the founder and president of computer security company NetDiligence, works with almost all major underwriters to assess companies' risks and recommend solutions. He believes that the market dynamic is changing and that interest in cyber policies is growing rapidly. At the same time, insurers are rushing in to compete in this marketplace, causing prices to fall and policies to become more standardized and a better value.

"Competition is getting fierce and we're now in a soft market that is great for buyers," he says. "However, the greater number of options available means that it is more fundamental than ever that your broker has detailed knowledge of the market. Your broker can make a huge difference," says Greisiger. "Policies can be complex, and the nuances of a policy can make them a much better fit for some companies than others," he says.

The level of protection you need is based not so much on the size of your company as on its activities. "Even if you are tiny you can still be sued, but if you are not engaged in ecommerce and your networks do not face customers, you might want to self-insure," Greisiger says.

Many companies fail to accurately identify their vulnerabilities because risk managers do not work closely enough with their IT departments to assess the risk and potential solutions. Another problem that risk managers run into is that treasurers still see cyber risk insurance as a "luxury cost issue," Greisiger says. However, the increasing publicity given to class action lawsuits stemming from the loss of electronic data is changing that perception. For more information on cyber risk insurance, please contact us.

PRODUCT*—continued from Page 4*

sense for only a few individuals. But as they became more popular, manufacturers added features, dropped prices and made them accessible to many. Until product liability wrap-ups become more common, you will want to evaluate a product liability wrap-up's coverage and costs against buying these coverages individually. Please contact us for more assistance in evaluating your product liability coverage needs.

REPUTATION*—continued from Page 1*

firm that specializes in crisis management can help your firm create contingency plans to deal with various scenarios. The hotel industry is a good example of preparedness. In a well-run hotel, every on-duty manager can access a binder with response guidelines for adverse events. Having well-considered responses ready will give you one less thing to worry about when dealing with a crisis.

For more information on protecting your firm's reputation, please contact us.

Product Liability: It's a Wrap

Wrap-up insurance has long been popular in the construction sector. Now wrap-up insurance is making inroads in the manufacturing and distribution sectors. Does a product liability wrap-up make sense for your firm? Here are some of the pros and cons.

Proponents of product liability wrap-ups say they can help retailers, importers, wholesalers, distributors and value-added manufacturers ensure that their product liability risks are predictable and manageable. But critics say that unless such owner-controlled insurance policies (OCIPS) are closely checked and administered, the owner can end up paying more for insurance — once for its direct liability risks and again for the suppliers' insurance.

Rupp's Insurance & Risk Management Glossary defines a wrap-up or OCIP as "Insurance… arranged by the owner…in such a way that all interests involved… are combined and insured under one policy with a single insurer. Generally, it includes workers' compensation, general liability, umbrella liability, and builders' risk insurance [for a construction wrap-up]; occasionally, it is only workers' compensation. It is designed to reduce the project's overall insurance costs and provide a coordinated project safety program."

Like a construction wrap-up, a product liability wrap-up is designed to meet the challenges of insuring a business that has complex relationships with its suppliers. While a construction wrap-up usually covers workers' compensation, general liability, umbrella liability and builders' risk, a product liability wrap-up might include product recall and product recall liability coverage, along with coverage for environmental liability, errors and omissions, crime and supply-chain disruption.

Foreign suppliers are often beyond the effective reach of the U.S. courts, dramatically increasing the distributor's risk of product liability claims. Further, many foreign suppliers don't fully understand the North American environment for product liability claims and often fail to purchase product liability insurance. Even if they do have insurance in place, they may have inadequate limits or policies with excessive limitations. The wrap-up helps protect the U.S. distributor by providing coverage for both the U.S. distributor and its designated foreign suppliers with one aggregate limit against product liability claims arising from the sale of foreign-made products.

A wrap-up can also eliminate some of the administrative hassles of a complex insurance program. U.S. distributors can find it hard to obtain valid certificates of insurance from their foreign suppliers, which might only provide a certificate with an expiration date. Securing a renewal certificate can be difficult if the distributor is no longer buying from the supplier and impossible if the supplier is out of business.

The product liability wrap-up is designed to solve these problems. Rather than requiring foreign suppliers to provide coverage — which might not be consistent — a product liability wrap-up provides distributors with coverage consistent with U.S. terms and conditions.

The cons

Because product liability wrap-ups are still relatively new, the concept often works better in theory than in practice. Arranging the proper coverage can be difficult to manage. And in the end, you might not save money if your suppliers' underwriters do not understand the concept. If your suppliers believe they need to retain their own product liability coverage, they may pass these costs on to you, so you in effect will be paying twice for the same coverage.

For now, you might be wise to consider a product wrap-up like a DVD player — when they were first introduced, buying one made

PRODUCT—continued on Page 3

Insurance is Good —Prevention is Better

Mark Greisiger, the founder and president of computer security company NetDiligence, points out that even the best insurance is never as good as preventing the problem in the first place. He identifies four main problems that drastically increase the threat to a company's data.

1. **Intrusion detection** – Most companies never know their data is compromised until they are informed by a third party.
2. **Poor encryption** – Companies rely on passwords, firewalls and biometric identification. But even with all these defenses, data must be encrypted where it resides – including on laptops used by outside salespeople.
3. **Data inventory** – Most companies never bother to run data audits that identify what information they have, where it is, and who has access to it.
4. **Porous perimeters** – Network defenses are only as strong as their weakest links. Companies should run regular tests that simulate hacker attacks and can identify vulnerabilities.

Tackling these four areas dramatically reduces risks and should enable companies to enjoy far better rates for cyber risk policies, Greisiger advises. "If you utilize 70 percent of best practices, you will get good rates," he says. "If you have 100 percent compliance with best practices, your broker will be able to shop you around. Companies will be fighting to offer you coverage." ■