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

Liability | Summer 2007 | Volume 17 • Number 3

Network Risks and How to Avoid Them

Computer-based risks ranked as the chief business concern among international corporate executives, found a survey by Swiss Re. Insurance and a sound risk management program can help you minimize the chances of concerns becoming crises.

Network risk insurance policies, offered by companies such as Aon, AIG, Fireman's Fund, Chubb and Ace USA, cover a wide variety of exposures. The most popular are third-party policies that provide customer notification services and credit monitoring as well as identity restoration for customers, employees and others affected by a data breach.

"Many state laws require businesses to notify individuals whose information has been compromised, and it's only a matter of time before a federal law is enacted," said Mike Roney, senior director, commercial business at Fireman's Fund.

However, even the best insurance is not as good as preventing a mishap in the first place. Responsible risk managers make sure they have in place a robust network defense system and a recovery plan.

The process can be divided into six broad strategies.

1 Define Risks and Quantify Threats

You need to identify the assets that need to be protected and assess what the potential damage would be in case of a breach. Would a breach cause the loss of identification record or loss of physical product? Would you incur legal liabilities or destroy customers' good faith? "Defining what you have to lose is the first step in building a proper security model and deciding where to allocate resources," says Timothy Mullen, a top computer security consultant.

2 Control Your Network

Every company must have a written corporate policy that defines what users can and can't do. The policy must be strongly enforced so that when IT staff find violations they can respond quickly. This policy will govern what workers can download and what programs they can install. Usually less will be better. Users should also never be allowed to run computers as an administrator. This will automatically limit the damage they might cause.

3 Stay Current

Budget for upgrades so that you have the most secure systems designed to meet the latest threats. Make sure that all the company's computers are patched with the latest software fixes on a regular basis. Remember that clean-ups after breaches far exceed the cost of upgrades.

4 Education

"A sustained educational campaign about the dangers of unsafe habits is essential," says Mullen. "Companies that do this will experience far fewer issues."

NETWORK—continued on Page 4

This Just In

Computer-based risks ranked as the chief business concern among international corporate executives, found a survey by Swiss Re. Despite this fact, only 25 percent of companies have a network risk insurance policy, according to the Insurance Information Institute.

Policies from various insurers can cover a wide risk of network-related exposures. In addition to buying insurance, there are other things you can do to minimize your risk of losses due to outage or penetration of your computer networks. See the article on this page for more information.

Vehicle accidents cause more work-related fatalities than any other cause. Statistics show those with prior driving offenses, even minor ones such as failing to stop at a stop sign, are more likely to be involved in an accident. Check candidates' motor vehicle records (MVRs) prior to hiring and conduct annual (MVR) checks for all those who drive on the job to see how your employees are doing on the road, both on the job and off.

The ABCs of Risk Management

Having a sound risk management plan not only protects a company from financial loss–it can help protect directors and officers from shareholder suits.

Ask any competent risk manager about their job and they'll tell you that it's as much an art as a science. Nevertheless, there are some clear strategies involved in the effective management of risk, starting with the basic need to identify and asses the risk of the organization and develop strategies for dealing with it.

There are many methods for identifying and assessing risk. One method looks at the source of the risk – for instance, weather events that could destroy property – while another looks at the problem itself – such as destroyed property, and analyzes what could cause it.

In general, most losses fall into six main categories:

- ✔ Property losses
- ✔ Business interruption losses
- ✔ Liability losses
- ✔ Key person losses
- ✔ Automobile losses
- ✔ Injury to employees.

Property losses can be caused by physical damage to property, loss of use of property or criminal activity. Damage could be caused to company buildings, contents, records and machinery. Exposures vary greatly from business to business and an experienced insurance broker can often be helpful in identifying your specific risk profile.

Business interruption losses could be the result of a property loss, action taken by authorities or a problem in the business supply chain. Liability losses could result from an accident on the premises or involving an employee on work time, a legal decision or a contractual dispute.

Identifying and assessing specific risks is actually the easy part of the risk management challenge. Once this stage is over the risk manager must decide how to deal with the identified risks.

There are four basic strategies to choose from: transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.

These strategies are often referred to as the 4 Ts:

Tolerate (retention)
Treat (mitigation)
Terminate (elimination)
Transfer (buying insurance)

Most risk management approaches use a combination of two or more of them. For instance, buying an auto insurance policy with a high deductible combines transfer with retention. Hiring a delivery service instead of operating your own truck fleet transfers the risk of operating those vehicles completely from your business. Alternatively, your company could decide that since its trucks are old, its drivers have great safety records and mostly use quiet rural roads where the risk of collision is small, the company can do without collision insurance and pay for any damages to the vehicles itself.

Mitigation can be achieved in many ways. Increasing the use of flame retardant materials in a building mitigates the risk of fire. Educating employees about workplace safety mitigates the risk of accidents.

Some risks can be eliminated entirely if they are judged too likely to occur, or too expensive to transfer, treat or tolerate. For instance, a company could decide to stop stocking a dangerous item and thereby terminate the risk of liability resulting from possible customer injuries. In one notable case last year the only maker of surfboard cores in the US decided to stop operations because it considered the risk of fire and health hazards was considered too large.

A host of factors affects the combination of strategies chosen. Most important among these factors are the financial resources of the organization, the organization's appetite for risk, the sophistication of its internal risk management and the tradeoffs of the insurance marketplace – how much it would cost to transfer the risk.

An organization's level of risk tolerance depends largely on its financial resources. It should never retain risk that could wipe out its net worth. It is also never a good idea to retain a level of risk that overly threatens its

ABCs—continued on Page 4

Why does YOUR company need a risk management policy?

Publicly traded companies need a formal risk management plan to protect their stockholders' investment. But even a privately held company needs to protect its stockholders' interests. Having a sound risk management plan can help defend the directors and officers from shareholder suits if the company loses value and nonparticipating shareholders allege mismanagement. ■

Preventing Heat-Related Illness

Heat stroke, the most serious heat-related illness, kills about 500 people a year in the U.S. ....Heat stroke is very serious and should be prevented at all costs. But other heat-related conditions have health and safety costs as well.

Summer brings warm weather—and increased danger of heat stress. Those who work outdoors are most vulnerable to heatstroke, particularly in summer months, but other work environments can also expose workers to excessive heat. These include commercial kitchens, laundries, chemical plants, foundries, and the like.

What health problems can heat cause?

Heat rashes are the most common problem in hot work environments where the skin is persistently wet with unevaporated sweat. Heat rash papules can become infected if not treated. Most heat rashes will disappear when the individual returns to a cool environment.

Heat cramps usually occur when performing hard physical labor in a hot environment. Cramps appear to occur due to excess salt build-up in the body when water lost through sweating is not replaced. Under extreme conditions, such as working for 6 to 8 hours in heavy protective gear, a loss of sodium may occur.

Heat stress occurs when heat generated by working muscles and heat from warm environments builds up in the body. When the body becomes overheated, blood goes to the surface in an attempt to cool the body, leaving less blood going to the active muscles, brain and other internal organs. Workers get weaker, become tired sooner and may be less alert, less able to use good judgment, and less able to do their jobs well.

Heat exhaustion results when the body is subjected to more heat than it can cope with. Body temperature and heart rate rise rapidly; a person experiencing this might not realize it because it involves no pain. An increase in body temperature of 2°F above normal can affect mental performance; an increase of 5°F can result in serious illness or death. Heat exhaustion symptoms include headache, nausea, vertigo, weakness, thirst and giddiness.

Heat exhaustion can also lead to heat collapse, where individual faints because his/her brain does not receive enough oxygen because blood pools in the extremities. Heat collapse occurs suddenly and can lead to injury if the victim falls or is operating machinery at the time.

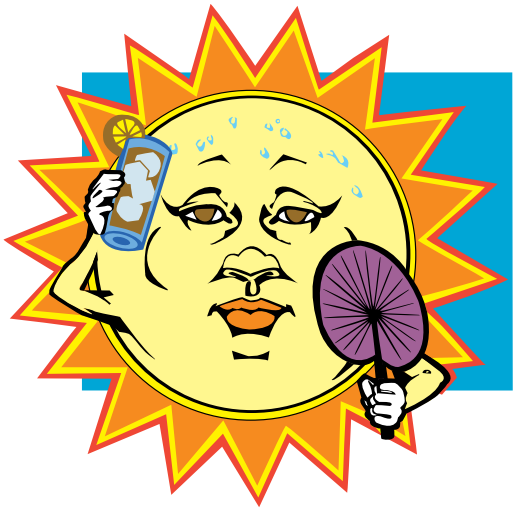
Heat stroke, the most serious heat-related illness, kills about 500 people a year in the U.S. Heat stroke occurs when the body's temperature regulation fails and body temperature rises to critical levels. Heat stroke's symptoms include confusion; irrational behavior; a lack of sweating (usually); hot, dry skin; and an abnormally high body temperature, such as 105.8°F (41°C). These can result in convulsions, coma and even death.

Heat stroke is very serious and should be prevented at all costs. More than 20 percent of people afflicted by heat stroke die, even young and healthy adults. Those who survive can become very sensitive to heat for months and experience varying degrees of brain and kidney damage.

Treating heat-related conditions

You can treat less severe heat-related conditions, such as heat cramps and heat stress, by allowing the affected worker to rest in a cooler, shaded location and drink cool, non-alcoholic liquids. Particularly in cases of heat cramps, drinking a carbohydrate/electrolyte drink can help replace minerals lost through perspiration. Changing into dry clothes will help those with heat rash feel better and prevent further skin irritation.

Heat stroke, however, requires immediate medical attention. If you suspect heat stroke, call for emergency medical help, even if the worker protests.



Preventing heat-related conditions

Avoidance is the best preventive measure for heat-related conditions.

For indoor environments, engineered solutions include improved ventilation, installation/upgrading of air conditioning, insulation of heat sources and increased conduction (movement of air) through fans or "swamp coolers."

For outdoor environments, reschedule work for cooler times of the day, such as early morning. Minimize heavy physical work, or spread it out over more workers than you would ordinarily use. Schedule water and rest breaks. Provide cooler recovery areas, where employees can rest in the shade or an air-conditioned space. Make water breaks mandatory, not optional. A worker in a hot environment should drink small amounts of water or other non-alcoholic beverages (about one cup) every 15-20 minutes. Cool liquids (50-60°) are best.

Workers in heavy or hot protective gear should periodically check their heart rate for signs of exhaustion. Have them count their pulse for 30 seconds at the beginning of each rest period. If the heart rate exceeds 110 beats per minute, they are excessively fatigued.

HEAT—continued on Page 4

SMART'S PUBLISHING

The information presented and conclusions stated in this newsletter are based solely upon our best judgement and analysis of information sources. It is not guaranteed information and is not necessarily a complete statement of all available data. Website citations are current at time of publication but subject to change. This material may not be quoted or reproduced in any form, including copy machines or any electronic storage or transmission medium, in whole or in part, without permission from the publisher. All rights reserved. ©2007 Smart's Publishing Group • 866-762-7879 (sales), 877-762-7877 (service) • www.smartspublishing.com.

HEAT—continued from Page 3

Shorten the next work period by one-third and maintain the same rest period.

Acclimatize workers who must be exposed to a hot environment gradually. NIOSH, the National Institute of Occupational Safety and Health, suggests that workers who have had previous experience in jobs where heat levels are high enough to produce heat stress may acclimatize with a regimen of 50 percent exposure on day one, 60 percent on day two, 80 percent on day three, and 100 percent on day four. For new workers who will be similarly exposed, the regimen should be 20 percent on day one, with a 20 percent increase in exposure each additional day.

Evaluate whether specialized cooling garments will work for your situation. These range from high-tech clothing, such as lightweight reflective gear (best in dry, high-heat or high-light environments) and circulating-air garments, to the relatively low-tech solutions of ice vests (filled with ice packs or dry ice) and wetting outer garments.

Train all employees on how to prevent and recognize the signs of heat-related illness. Educate them on the dangers of using alcohol in hot environments. Have employees on prescription drugs check with their physicians to see if they increasechances of heat fatigue.

Train at least one member of each work crew in first aid and CPR. Have a complete first aid kit available at every work site.

For more information on preventing heat-related or other occupational illnesses, please call us. ■

Other Health Factors

Factors besides hot environments can increase the chances of heat-related health problems. These include:

- ✔ Age – older workers are more susceptible
- ✔ Excess weight
- ✔ Lack of physical fitness
- ✔ Lack of acclimatization
- ✔ Dehydration
- ✔ Protective gear that inhibits heat loss
- ✔ Prior heat injury
- ✔ Hypertension (high blood pressure)
- ✔ Use of alcohol or certain drugs

Not just a health problem

In addition to creating serious, immediate health problems, heat can affect safety and health in less obvious ways. Accidents appear to occur more frequently in hot environments than in more moderate conditions. Heat can impair physical performance and lower mental alertness. Increased body temperature and physical discomfort can also cause workers to become irritable or angry, which can distract attention from hazardous tasks or cloud judgment. Heat can also promote accidents by causing palms to become sweaty and slippery, by causing dizziness or causing safety glasses to fog. ■

ABCs—continued from Page 2

cash flow or profits, especially if it's a public company where an adverse earning report could have a disproportionately high impact on the stock price.

A sophisticated risk management team – which could include in-house professionals, along with outside experts such as insurance agents, accountants or actuaries and attorneys – will be able to ensure that the company's level of risk remains in the desired parameters. Every organization also needs a business continuity plan in place to ensure optimal recovery from disruptive events. ■

NETWORK—continued from Page 1

5 Divide and Rule

Make sure that your computer system is segregated so that a breach in one area does not allow access to the entire network. Operate on a system of least privilege – only give people the networking rights they need to do their job. Ensure that mobile users have encryption and strict access controls so that a lost laptop cannot compromise the entire system. "Make a lost laptop a $1,000 dollar issue, not a $1,000,000 issue," says Mullen.

6 Plan for Disasters

Make sure you have a recovery plan in case security is breached. What insurance do you have, what backup data systems, which personnel are on call to minimize the impact of any disruption?

For more information on the insurance coverages available, please contact us. ■

The Ten Steps Towards Better Business Insurance

It's easier than you think to save money on business insurance and get better coverage at the same time.

1. Check on insurer solvency with companies like Moody's before purchasing a policy.
2. Read your policy. Make sure it covers the replacement cost of the property and consider buying "building ordinance coverage," which pays to rebuild to current building codes.
3. If you lease your premises, take out a renter's commercial policy and make sure that there is a mutual waiver-of-subrogation clause in your lease.
4. Ensure that your independent contractors carry their own workers' compensation and liability insurance.
5. Keep a list of all of your business property, both at work and somewhere off the premises.
6. Don't hide unusual risks from your agent.
7. Inform your agent of changes to your business, so that you and your agent can discuss coverage options.
8. If an employee uses his vehicle for your business, you should discuss business auto coverage options with your agent.
9. Compare your coverage and liabilities with other businesses in the same field and determine the average legal costs and settlements to set your coverage limits.
10. Try to find a business package policy that fits your situation. These policies, which combine property and liability coverages, will usually result in savings. But be sure to understand the extent of coverage. For instance, most professionals will require a separate errors & omissions policy. ■