Managing Risk

MORTON
INSURANCE & RISK MANAGEMENT

7340 East Caley Ave., Suite 350 • Centennial, CO 80111
Phone: 877.836.2660 • Fax: 720.488.4918 • www.mortonriskmanagement.com

Winter 2007 Volume 17 • Number 1

Protecting Your Company from Liability for Data Breaches

Preventing a data breach costs much less than correcting it.

The U.S. Office for Victims of Crime estimates that identity theft has affected 27 million individuals over the past five years. Identity theft and identity fraud refer to crimes in which someone wrongfully obtains and uses another's personal information for fraudulent purposes, typically for economic gain.

For victims, ID theft is costly in terms of money, time and emotional strain. According to Forbes.com, "The Privacy Rights Clearinghouse estimates that victims on average spend the equivalent of 22 work days cleaning things up." (ID Theft Insurance Isn't Insurance, 5-29-03)

To commit their crimes, ID thieves use personal identifying information such as Social Security numbers, bank account or credit card numbers, telephone calling card numbers, and other valuable identifying data. So where do they get this information? *From businesses like yours.* The Privacy Rights Clearinghouse, a consumer advocacy organization in San Diego, estimates that companies and institutions have collectively "fumbled" some 93,754,333 private records, according to a recent *New York Times* report.

ID theft costly to businesses, too.

ID theft ends up costing not only the victims, but the organizations where the information breach occurred. Risk exposures include:

- **Liability.** According to PLUS, the Professional Liability Underwriting Society, the number of privacy lawsuits has increased 300 percent in the last 10 years.
- **Fines.** Many federal laws govern privacy and call for penalties when an organization fails to take appropriate steps to protect individuals' personal identifying information.
- **Notification costs.** At time of publication, 29 states had laws requiring businesses and nonprofits to notify their clients when their personal information is breached. These states include: Arkansas, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, Washington and Wisconsin. Laws will take effect in Kansas, New Hampshire and Utah on January 1, 2007. Standards for notification vary by state—stricter standards, such as California's, call for notification for any breach. Less-strict standards require notification only if a risk of identity theft exists. For details on state laws, see the State PIRGs (Public Research Interest Groups) site at www.pirg.org/

DATA—continued on Page 4

Risk Notes

E-crime incidents are declining, but the financial impact is up, found a *CSO* magazine survey. Respondents (primarily larger organizations) reported an average of 34 "security events" from July 2005 to June 2006, down from 86 during calendar year 2005. However, financial losses averaged $740,000 during the July 2005-June 2006 period, up 45 percent from 2005. The survey defined e-crime as automated attacks (such as viruses, worms and malicious code; unauthorized access or use of information systems or networks; spyware and illegal generation of spam) and targeted attacks, such as theft of proprietary information, system sabotage and theft of intellectual property.

Preparing for Pandemics

The World Health Organization says a pandemic could debilitate up to 25% of the workforce at one time. How will your business survive?

The U.S. hasn't seen a major pandemic since the Hong Kong flu, which caused 35,000 deaths in the U.S. in 1968. However, in a world where air travel brings 1.6 billion people across international borders each day, a highly infectious strain of influenza could become a global problem in a very short time.

Pandemic flu differs from ordinary "seasonal" flu viruses. Pandemic flu is a virulent human flu that causes a global outbreak, or pandemic, of serious illness. Pandemic flus generally occur when a virus ordinarily found in animals mutates and spreads to humans. Because people have little natural immunity, the disease can spread easily. Currently, there is no pandemic flu, although public health experts are keeping a careful eye on the avian flu, warning that it could mutate into a form that spreads more easily.

If a flu pandemic occurs, public health experts estimate it could kill 200,000 to 1.9 million people in the U.S., and 180 million to 360 million people worldwide. Loss control experts agree that businesses are woefully unprepared for dealing with this type of crisis. Businesses themselves agree: in a survey released in December 2005, "…66 percent of respondents said their company had not adequately planned to protect itself from a pandemic flu outbreak, while 14 percent said they had adequately planned and 20 percent were undecided." (Source: Deloitte Center for Health Solutions)

Some considerations for employers:

- In event of pandemic, people of working age will be hit the hardest. Unlike seasonal flus, which primarily affect the young, the old and those with weakened immune systems, in past flu pandemics, 20- to 30-year-olds suffered the highest death rates. The World Health Organization (WHO) estimates that pandemic may debilitate up to 25 percent of the workforce at any one time.
- Vaccines will be ineffective. According to the Centers for Disease Control, a vaccine's ability to protect depends on the similarity or "match" between the virus strains in the vaccine and those in circulation. As pandemics occur when new or rapidly mutating viruses spread, existing vaccine stocks will not work—and it takes six months or more to develop new vaccines.
- Public health quarantines may occur, preventing workers and customers from coming to your business premises.
- Quarantines on imports may also be imposed. Even without quarantines, worker shortages and travel restrictions might interrupt the delivery of goods and materials your business needs.

Insurance considerations

Unfortunately, there's little coverage available for pandemics. Business income policies typically pay only when insured loss or damage to covered property causes a business interruption, so your policy likely will not cover income lost due to pandemic. Nor will contingent business interruption policies cover you if a pandemic closes or slows production at a "dependent location," such as a key supplier or vendor. (Some Canadian companies are developing coverage for pandemics; however, to date no American companies offer this coverage.)

A pandemic could also affect your benefits program. Pension plans that pay death benefits could face liquidity problems if death rates increase. Businesses that self-insure employee medical benefits could drain their cash flow.

Your workers' compensation program is unlikely to face pandemic-related claims, unless you are in the healthcare industry, since workers' compensation covers only work-related illnesses.

Directors and officers of publicly traded companies could face liability claims if the company experiences pandemic-related losses and shareholders allege they did not adequately prepare. Your directors and officers liability (D&O) policy may cover this type of claim. However, the best policy is to prevent this type of claim from occurring by taking reasonable steps to prepare for a pandemic.

Action steps:

1 Update your emergency procedures (you do have written ones, don't you?) to include what to do if pandemic causes widespread illness or quarantines.

2 Because flu victims generally are contagious for several days, develop flexible sick-leave policies to encourage sick employees to stay at home and avoid spreading illness.

3 If you self-insure medical benefits, make sure you have adequate stop-loss insurance.

4 Identify all employees whose jobs (or essential functions thereof) could be performed at home or off-site. Develop a telecommuting program that would allow these people to work at home in event of emergency. Work with IT staff to get sys-

PANDEMIC—continued on Page 4

Workers' Compensation, Safety and Multiple-Injury Employees

Multiple injuries could indicate a worker hasn't completely healed...or a safety problem.

In an article in the *Chicago Sun-Times* (October 19, 2006), the author quoted an employee with numerous workers' compensation injury claims who said that "the city is a dangerous place to work." With more than $340,000 received in claims payments over his tenure, the employee said his injuries were a direct result of other workers not being careful. In one example, he said that mechanics left oil on the floor of the shop, which caused him to slip and fall numerous times while attempting to clean up. Apparently it did not occur to the worker that he had a responsibility toward maintaining a safe working environment, as well.

Human resources and the safety department need to make a joint effort to identify and correct problems related to multiple-injury employees. Everyone shares the responsibility of correcting workplace hazards, which include improper employee practices. This includes managers, supervisors and front-line employees participating in hazard recognition and removal.

Review the injury database and find those employees who have had numerous reported injuries, whether they have taken workers' compensation benefits or not. One steel mill reviews injury reports every month, and any person having three or more injuries—regardless of severity—is identified and meets with their supervisor and department manager to discuss the importance of safe performance and the employer's expectation that the employee will follow procedures. Continuing to make the list will lead to probation, up to and including termination. One manager states it this way: "Sometimes we have to protect people from themselves as well as others."

About 70 percent of injuries are directly related to housekeeping issues. Poor housekeeping reflects poor work habits as well as poor management skills. Get a handle on improving housekeeping and numerous hazards will go away. Communicate with your employees the importance of maintaining a safe and productive work environment and each employee's responsibility for doing so.

Also communicate with your managers about their responsibility to help their employees meet expectations. A mechanic who walks away from an oil spill he created is not doing his job; another employee who sees the hazard and walks through it or ignores it is not doing his job; and a manager who condones sloppy or incomplete work and provides little or no guidance to the employee is not doing her job.

So how do you get everyone to participate in eliminating hazards? Don't start with the "Because OSHA says so" philosophy. Instead, communicate why something is dangerous and why it's important to eliminate or reduce the hazard.

Train employees and managers in hazard recognition. Too often the safety professional identifies what may be an obvious hazard while employees continue to work around it unrecognized. Once employees know what to look for, they can correct or remove it.

Encourage employees to take initiative to correct identified hazards through a safety recognition program. It doesn't have to cost much but it will save you profits, time and employees in the end. Also, include safe performance as an accountability factor equal to attendance, quality of work and other measured factors. What counts is not eliminating injuries, but performing tasks the right way.

Train your managers in their roles and responsibilities, helping them to understand the value of their front-line duties with employees. Observation skills, interpersonal skills and accountability are all essential in daily interaction with employees.

When everyone works together toward recognizing and eliminating hazards, synergy occurs and the work environment improves. Employees change unsafe conditions and unsafe or at-risk practices, and fewer opportunities for injuries to occur arise. This lowers the number of injuries, which lowers workers' compensation claims and costs. You'll save dollars and lives as a result. ■

DATA—continued from Page 1

consumer/credit/statelaws.htm.

So, what does notifying customers cost? A survey by the Ponemon Institute found that each lost record costs companies an average of $140, for a total of $5 million in direct costs per incident.

✹ **Public relations costs.** A breach of customer information can damage an organization's reputation. Another study by the Ponemon Institute found that, of the 23 million U.S. adults who have been notified of a breach of their personal data, approximately 20 percent terminated their accounts and another 40 percent were considering it. Adverse publicity from the breach will likely impact sales as well.

How do you minimize the risk of data breaches?

To protect your business from liability for data breaches, familiarize yourself with privacy laws. Federal laws governing the security of private consumer information include:

✹ **Family Educational Rights and Privacy Act of 1974** (FERPA): Applies to educational institutions and agencies that receive federal funding.

✹ **Fair Credit Reporting Act** (FCRA): Applies to credit reporting agencies and credit bureaus.

✹ **Financial Services Modernization Act** (Gramm-Leach-Bliley): Applies to financial institutions.

✹ **Video Privacy Protection Act of 1998:** Applies to video rental or sales outlets.

✹ **Health Insurance Portability and Accountability Act of 1996** (HIPAA): Applies to health plans (including self-insured employers), health care clearinghouses and providers.

✹ **Children's Online Privacy Protection Act** (COPPA): Applies to almost all commercial Web sites and online services, requiring them to obtain parental consent before collecting personal information from children under 13.

✹ **Fair and Accurate Credit Transactions Act:** Applies to any business or individual who uses consumer information for business purposes. The Act requires consumer information to be disposed of properly to prevent "unauthorized access."

Action steps you can take to minimize your exposures include:

✹ Ensure your IT department uses the latest technology to secure data and networks, and prevent unauthorized personnel from accessing your systems.

✹ Avoid using employee Social Security numbers for identity numbers and limit access to employees' private information—including information on medical conditions, claims and disabilities—to a need-to-know basis. Ensure that this information is stored on secure systems, and that those with access to it log off their computers when away from their desks.

✹ Dispose of any records containing personal data properly. Shred printed records before discarding. And when disposing of any electronic media (including hard drives), either destroy the media or reformat it—when you simply "erase" data, it just gets overwritten and can be recreated.

✹ Consider buying one of the new identity theft policies for businesses. These policies protect your firm from liability losses when your data is stolen or used by identity thieves. Policies cover direct expenses, such as defense costs, legal damages, fines, regulatory actions and notification costs. Some policies also cover services that protect or help restore your reputation, including public relations counsel and assistance for victims. Group policies that protect your employees from the costs of identity theft are available as well. ■

PANDEMIC—continued from Page 2

tems in place to allow telecommuting.

5 If a pandemic occurs, have nonessential employees stay at home. Avoid gathering large groups together in enclosed spaces, such as meeting or conference rooms. Substitute telecommunications wherever possible for face-to-face contact.

6 Educate employees on proper sanitation to prevent the spread of disease. This includes washing hands after sneezing, coughing or using the bathroom and before and after eating, and staying home when ill. Those whose immune systems are compromised might want to wear facemasks when in public. ■

Driving While Distracted

Using a cell phone could impair driving as much as drinking, found a study published in Human Factors: *The Journal of the Human Factors and Ergonomics Society.* The study tested responses of 40 volunteers on driving simulators while undistracted, while using a handheld cell phone, while using a hands-free phone and while intoxicated to a .08 percent blood alcohol level, the average for being legally considered impaired in the U.S.

The study found that both intoxication and cell phone use impaired reflexes. Drivers using a cell phone drove and responded more slowly to events and were more likely to be involved in an accident. Drivers who were intoxicated also drove more slowly but more aggressively, requiring them to brake harder. Although none were involved in an accident during this study, the link between intoxication and accidents has been proven many times. Interestingly, the study found no difference in reaction time between drivers using handheld vs. hands-free cell phones. ■

New WC Risks

According to the Insurance Information Institute, new risks emerged for workers' compensation during 2006. These include: workers with limited English language skills and undocumented workers, who have high incident rates of injuries and fatalities (especially pronounced in Latino workers); the latent risk associated with first responders working major catastrophes, who show high frequencies of respiratory ailments along with "traditional" injuries; and the problems of re-integrating returning veterans, who may have physical and psychological injuries, into the workforce. ■