MANAGINGRISK

"Companies get out in front and stay there by raising the standards by which they judge themselves and by which they are willing to be judged."

—Fred Smith

Morton Insurance & Risk Management

7340 East Caley Ave., Suite 350
Centennial, CO 80111

Phone: 877.836.2660
Fax: 720.488.4918

www.mortonriskmanagement.com

RISKNotes

Computer viruses cost U.S. organizations $55 million in 2003, according to the 2004 Computer Security Institute (CSI)/FBI Computer Crime and Security Survey. Denial-of-service attacks, where hackers disable networks by flooding them with useless traffic, cost $26 million. Proprietary data theft came in as the third most costly computer crime, at $11.5 million.

Until April 30, employers must post a summary of their prior-year injuries and illnesses, according to a rule by the U.S. Occupational Safety and Health Administration (OSHA). The rule requires most employers with more than ten employees to post form 300A, the Summary of Work-Related Injuries and Illnesses, at their worksite from February 1 to April 30. The form is part of the OSHA booklet, "Forms for Recording Work-Related Injuries and Illnesses." Even those employers with no work-related injuries or illnesses must post the summary form, with zeroes in the spaces for recording injuries and illnesses. See www.osha.gov/recordkeeping/new-osha300form1-1-04.pdf for a copy of the booklet.

ALSO IN THIS ISSUE

Property

Fire Prevention

Risk managers today have to deal with all kinds of exposures that were unheard of a generation ago. Cyberextortion; identity theft; sexual harassment and compliance with the Americans with Disabilities Act, Sarbanes-Oxley and other laws cause risk managers many sleepless nights.

Despite that, one of the oldest hazards known to mankind still affects businesses today—fire. Improvements in building materials and stricter building codes have reduced the danger of fire spreading from one building to another, yet structure fires still caused more than $8.6 billion in property damage in 2003, according to the U.S. Fire Administration. Although the majority of structure fires occurred in residential buildings, $2 billion of damage occurred in non-residential buildings in 2003. Of that $2 billion, $721 million in damage occurred to store and office properties and $675 million occurred in storage properties. As you can see, fire remains a significant risk exposure for business owners.

Protecting your business from fire

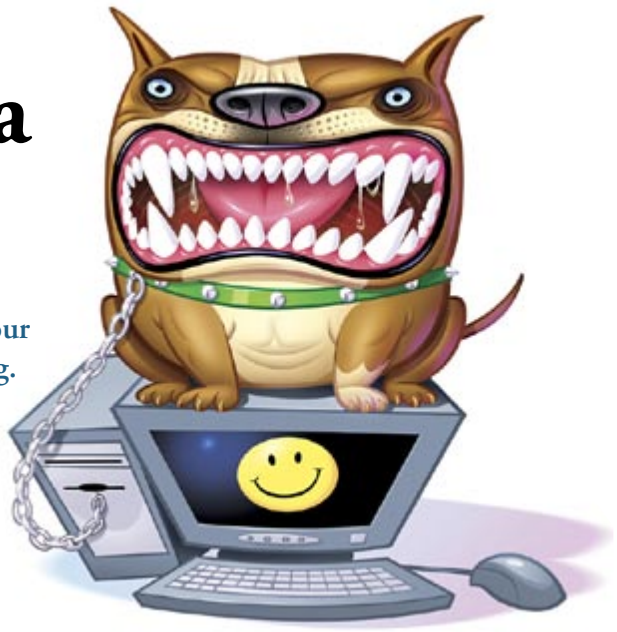
Fires need tinder, or easily combustible materials, and oxygen to start. If a spark, electrical short, excess heat or other ignition source contacts tinder where oxygen is present, a fire will likely start. Whether it spreads depends on the amount of oxygen and fuel available. Preventing fires therefore requires ensuring that combustible materials do not come into contact with ignition sources. And to contain or slow the spread of fires, you need to minimize their contact with additional fuel sources and oxygen.

A fire can start inside or outside your structures. To begin a fire prevention program, check the perimeter of the building for the following:

- ✔ Flammable debris, such as paper, rags, wood, trash. If you must store these items near your structures, store them in solid containers, the more airtight the better.
- ✔ Flammable liquids. Make sure any flammable liquids stored outside your structures, including propane and other fuel tanks, are well-labeled and securely closed. In certain areas, you might need to store these in a fenced, locked area.
- ✔ Landscaping—well-maintained landscaping can help prevent the spread of fires. Mature shrubbery is somewhat fire-resistant. Weeds, on the other hand, grow and burn quickly. If your property has overgrown areas, consider planting (and maintaining) these areas, or clearing them and replacing planted areas with hardscaping.

FIRE — continued on Page 3

Why You Need a Data Management Policy



In recent years, many of our articles have discussed how to protect your company from the loss of data, whether through fire, theft or hacking. However, the storage of data can also create some risk exposures. Read on to find out why—and what you can do about it.

Data as evidence

It has become routine for plaintiffs' attorneys to request any and all documents, print or electronic, even remotely related to a case. For example, if an employee makes charges of sexual harassment against a company, the attorneys often request copies of all e-mail messages sent by the defendants in an attempt to prove a pattern or culture of sexual harassment. Sometimes these "fishing expeditions" turn up circumstantial evidence that can bolster a case—a joke in poor taste, an off-the-cuff remark—that might have more to do with the informal nature of e-mail than any pervasive pattern of harassment. Nevertheless, these records can cause damage. Electronic records have also played an important role in other investigations, including those for securities fraud and patent infringement.

However, routinely destroying or deleting e-mails and other electronic files also creates its own exposures. Businesses that use computers to manage projects, such as software development or construction projects, face special data management challenges. These companies might need to access archival records of a project to support defense if accused of patent infringement (in the case of a software company) or defective construction (in the case of a contractor). Further, defendants in a lawsuit might be accused of "spoliation of evidence," a tort, if a haphazard or nonexistent data destruction policy causes them to destroy relevant documents after the filing of a claim.

Sarbanes-Oxley presents new challenges for publicly traded companies. Formally known as the Public Company Accounting Reform and Investor Protection Act and enacted in July 2002 following the Enron and other accounting scandals, Sarbanes-Oxley imposes new controls on accounting and recordkeeping. This wide-ranging law contains three provisions of particular interest to information officers and those who manage documents: 1) Section 302 —Corporate Responsibility for Financial Reports, which requires executives to personally verify the accuracy of financial reports, 2) Section 404 — Management Assessment of Internal Controls, which requires executives and auditors to attest to the effectiveness of internal controls and 3) Section 802 — Criminal Penalties for Altering Documents, which outlines requirements for the protection and retention of financial audit records. Compliance with Sarbanes-Oxley is beyond the scope of this publication, so if your business is a public corporation, please contact your auditing firm or attorney for more information.

Some key points in developing a data management policy:

- Get key departments involved—information technology, finance, compliance and senior management, along with your attorney, auditing firm and insurance broker.
- Determine storage criteria for critical documents. What documents do you need to keep and how long do you need to keep them? Even private companies should store tax-related documents for a minimum of seven years, in case of audit. Requirements for publicly traded companies are more formal—contact your accounting firm for information. Other documents—such as internal memos and project documentation—might not have specific requirements, but should be stored as long as you might need them. Examples of documents to store indefinitely would be copies of old insurance policies, information on possible insurance claims or litigation, and the like. You will want to develop your own criteria for the storage of project-related documents, depending on your company's exposure to product liability, copyright or patent infringement and other claims.
- Determine storage criteria for nonessential documents, such as informal internal communications and e-mails. You might not need to retain these archives for more than six months or so—whatever you use as a criterion, be sure to implement it consistently.
- Document how and when you will destroy unneeded documents and develop a plan for suspending this policy if you need to retain documents for evidence in a lawsuit.
- Determine how you are going to store electronic records you need to preserve. Changing technology makes this an important question for your IT department to address—will you have the software and hardware needed to locate and access specific documents in two years? In five? In 10? When updating software and systems, you might want to retain copies of "archival" software or, alternatively, store documents in a text-only format.
- Determine whether your existing insurance coverage is adequate to cover your new exposures due to Sarbanes-Oxley and other laws. For more information, For more information, please contact us. ❑

The Ten Biggest Mistakes Employers Make (and how EPLI can help)

Employment-related lawsuits have increased dramatically in the last 15 years. In 1990, plaintiffs filed 8,272 employment civil rights complaints in US district courts. By 2000, that number had increased to 21,032—a jump of more than 150 percent. This doesn't include all the employment discrimination or wrongful termination claims filed in other jurisdictions or settled out of court.

All employers face employment-related exposures, but some practices can increase your vulnerability. Here's a list of the most common employment-related mistakes employers make, with suggestions for avoiding them:

1 **Failing to understand, and comply with, federal civil rights and privacy laws.** These include:

- Title VII of the Civil Rights Act of 1964 (Title VII), which prohibits employment discrimination based on race, color, religion, sex or national origin;
- Equal Pay Act of 1963 (EPA), which protects men and women who perform substantially equal work in the same establishment from sex-based wage discrimination;
- Age Discrimination in Employment Act of 1967 (ADEA), which protects individuals who are 40 years of age or older;
- Title I and Title V of the Americans with Disabilities Act of 1990 (ADA), which prohibits employment discrimination against qualified individuals with disabilities in the private sector, and in state and local governments;
- Civil Rights Act of 1991, which, among other things, provides monetary damages in cases of intentional employment discrimination; and the
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), which protects individuals' personal health information.

A qualified human resource professional or employment attorney, whether on staff or a consultant, can review your company's HR policies and procedures to ensure compliance. 2 **Failing to realize your state might provide additional civil rights and privacy protections.** Many states have laws that go beyond federal law in protecting workers' civil rights, including prohibiting job discrimination on the basis of sexual orientation, as well as stricter privacy protections. Staying abreast of all these laws can be difficult, particularly if you operate in more than one state. Again, a qualified human resource professional or employment attorney can help.

3 **Failing to develop a policy on sexual harassment.** According to Best's Review, the "typical" Fortune 500 company spends $6.7 million a year, or $282 an employee, on sexual harassment each year. These larger companies could buy "meaningful prevention" programs at only $200,000, or $8 an employee. Even smaller companies face potentially crippling expenses: defense costs alone for a "routine" sexual harassment lawsuit range anywhere from $55,000 to $150,000 or more. To prevent sexual harassment, include statements in your employee handbook prohibiting sexual harassment, including examples of what constitutes "unwelcome sexual advances" and a "sexually hostile work environment" and outlining your company's complaint and disciplinary procedures. Employers that have had complaints of sexual harassment need a stepped-up prevention program, including offering sensitivity classes to supervisors and managers.

4 **Making layoffs without planning.** Improperly handled layoffs offer fertile grounds for wrongful termination class action suits. When making a layoff, ensure it won't disproportionately affect any protected classes of employees, such as women, minorities and those over age 40.

5 **Failing to document performance problems or disciplinary actions.** Even when you have cause to terminate an employee, you could face a wrongful termination suit if you lack documentation. To prevent this, train supervisors to document all violations of company rules and resulting disciplinary actions. Conducting regular performance reviews and maintaining written records, signed by the supervisor and employee, can also help you spot recurring performance problems and help you make the case for termination, if needed.

6 **Asking job applicants about their medical history or requiring them to take medical exams.** The Americans With Disabilities Act (ADA) prohibits asking applicants about their disabilities or requiring medical exams before offering employment. Employers can ask applicants if they can perform the "essential duties" of the job, with or without "reasonable accommodations." Once you make a bona fide job offer, you can ask applicants to take medical

MISTAKES — continued on Page 4

FIRE — *continued from Page 1*

Fires can start inside a building as well. Potential fire starters you can find in your building include:

- ✔ "Ordinary" combustibles, such as paper, wood, cloth, rubber, building materials. Storing these materials in appropriate containers can minimize their potential to become fuel in a fire.
- ✔ Flammable liquids, such as fuel oil, gasoline, cooking oils, solvents. Again, storing these liquids in properly sealed containers can prevent problems.
- ✔ Electrical equipment, such as wiring, fuse boxes, motors. Minimize your fire risk by having only qualified contractors install or repair wiring. Keep motorized equipment well-maintained and clear of any combustible debris.

To contain a fire once it begins requires the proper equipment. Every business, no matter how small, needs at least one fire extinguisher per floor. One fire extinguisher will not work on all types of fires. For best results, match the type of extinguisher to the type of combustibles in the area:

- ❑ **Class "A"**– Ordinary combustibles (wood, paper, cloth, rubber, etc.)
- ❑ **Class "B"**– Flammable liquids (fuel oil, gasoline, cooking grease, solvents, etc.)
- ❑ **Class "C"**– Energized electrical equipment (wiring, fuse box, electric motors, etc.)
- ❑ **Class "D"**– Combustible metals (magnesium, sodium, zirconium, etc.)

Train employees on fire safety. The following tips can minimize injury and property damage:

1. Appoint someone to check smoke detectors and fire extinguishers on a regular schedule, at least twice a year. Sprinkler systems also need periodic professional inspections; check with your installer for information.
2. Learn how to use a fire extinguisher properly. Pull the pin, aim at the base of the fire, squeeze the handle and spray from side to side at the base of the fire. For safety, the operator should stand between the fire and the exit to allow a quick escape if the fire does not go out.
3. If anyone's clothing or hair catches fire, train them to immediately stop, drop and roll. Running will only feed the fire, causing it to burn more intensely and spread.
4. If trapped inside, prevent smoke from spreading by closing doors, blocking any gaps underneath with towels or cloth – preferably wet, if water is available, and covering mouths and noses with cloth.
5. If a small fire threatens to spread or the room becomes smoky, evacuate immediately and call 911. An untrained person should never try to fight a large fire.
6. Ensure your property is protected with adequate insurance limits. For more information on protecting your property from fire, please call us. ❑

MISTAKES — *continued from Page 3*

exams, as long as they focus on the applicant's ability to perform the job.

7. **Failing to recognize increased religious diversity.** Title VII of the Civil Rights act prohibits discrimination or harassment on the basis of religion, in addition to race and gender. Employers must accommodate workers' religious beliefs, unless it would create an undue hardship to the business. This might mean giving workers religious holidays off, allowing time off and a quiet place for prayers or bending dress codes to allow the wearing of traditional attire.

   Proseletyzing at work can cause other problems. Employers must walk a fine line between upholding the proseletyzer's rights to free speech and other employees' rights not to be harassed on the basis of religion. A case-by-case approach works best, but any claims of harassment or intimidation need investigation.

8. Violating employees' medical privacy. HIPAA protects "individually identifiable health information….created or received by a health care provider, health plan, employer, or health care clearinghouse [that]…relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual…" Employers might have access to employees' medical information when determining physical capability for a job, providing health benefits, providing workers' compensation benefits, determining eligibility and appropriateness of return-to-work assignments, and in determining eligibility for medical leave benefits. Limit access to these medical records to those with a need to know for administrative purposes.

9. **Failing to have the needed insurance coverage.** General liability policies exclude employment-related claims. Although most directors & officers (D&O) policies will cover employment practices claims, they only cover directors and officers named in the suit. The corporation itself will not have coverage, unless your D&O policy contains "entity coverage." This still leaves non-directors and officers uncovered.

   Employment practices liability insurance (EPLI) protects employers from employment-related claims by covering both your legal defense costs and any settlements you might have to pay in an employment-related case. It protects employers from claims by employees, job applicants and past employees that the employer violated their legal rights.

10. **Neglecting to have adequate EPLI limits.** In 2003, the median compensatory jury award for employment-practice liability cases (including wrongful termination and all types of discrimination) rose to a nationwide median of $250,000. The median compensatory jury award for discrimination cases alone was $235,000. Although EPLI can be expensive, it can save you thousands or even millions. Look for a policy that offers separate limits for defense—attorney fees for a complex or class action suit can often eat up your limits, even before you have to pay any settlements.

For more information on reducing your employment practices liability exposures, please call us. ❑