Managing Risk

ZINN
Clear direction from a trusted source
www.zinn.com

Myerstown Office:
16 East Main Avenue
Myerstown, PA 17067
717-866-5717

Lebanon Office:
761 Poplar Street
Lebanon, PA 17042
717-272-6693

Cut Costs by Managing Double Dipping

Workers' compensation pays injured workers only a portion of their pre-injury salary while they recuperate. And there's a good reason for that—if an injured worker receives as much for staying at home, why return to work?

In most states, workers' compensation benefits replace two-thirds of a totally disabled worker's pretax earnings, subject to a maximum. This gap gives employees incentive to return to full-time, productive work.

Why Is Double-Dipping a Problem?

Keep in mind that employees receive workers' compensation benefits tax-free, and they also save on commuting and other work-related costs. When a worker receives other benefits due to their disability (called double dipping), their total benefits can approach or even exceed their pre-disability earnings. This gives them little incentive to return to full-time productive work.

What Employers Should Look for

Employers will want to ensure that an injured or ill employee receives the benefits due him or her, without becoming overinsured. Fortunately for employers, most health and disability insurance programs, including Social Security disability,

Risk Tip

OSHA's Top Ten for 2013

Every year, OSHA releases a list of its top ten most frequently cited violations of workplace safety and health codes. The list for 2013 follows:

1   **Fall protection (C)**
2   **Hazard communication**
3   **Scaffolding (C)**
4   **Respiratory protection**
5   **Electrical: wiring**
6   **Powered industrial trucks**
7   **Ladders (C)**
8   **Lockout/tagout**
9   **Electrical: systems design**
10 **Machine guarding**

C = Construction standard; applies to construction businesses

OSHA publishes this list so employers can find and fix recognized hazards before OSHA shows up for

have coordination of benefits provisions. These provisions prevent overinsurance by reducing the benefits the policy will pay by amounts the claimant receives from other sources, including workers' compensation.

Possible sources of overinsurance include the following:

Group long-term disability policies: The typical disability policy provides a monthly benefit equaling 60 percent of the employee's pre-disability wages, subject to a maximum. When coupled with workers' compensation lost-time benefits, total monthly benefits could exceed a disabled worker's pre-disability earnings. If your organization offers group disability income benefits, make sure your plan includes a coordination of benefits provision. Most (but not all) individual disability policies also contain coordination of benefits provisions. Most also discourage malingering by requiring an insured to accept "any gainful employment" he/she is "reasonably suited to" by education and experience after a certain period, such as two years, or forfeiting benefits.

Social Security disability insurance (SSDI): Social Security pays disability benefits only for total and permanent disability. Totally disabled workers can receive benefits under both SSDI and workers' compensation, but Social Security will reduce the amount of any benefits paid by amounts received from workers' conmpensation. The combined total of workers' compensation and SSDI benefits cannot exceed 80 percent of the worker's average current earnings.

Unemployment benefits: Each state has different criteria to determine eligibility for unemployment benefits. Some require an employee to be able and available to work to receive benefits, which would exclude anyone out on work-related disability. Others will pay unemployment benefits to workers receiving workers' compensation benefits under certain circumstances. If your state allows this, your organization should offer all injured workers transitional jobs that take into account their physical limitations. Workers who refuse these jobs will likely be deemed ineligible for unemployment benefits.

Sick leave: Take a look at the structure of your sick leave program. Many employers allow employees to use sick leave, vacation leave and personal leave to supplement their workers' compensation benefits. You'll want to ensure these plan documents contain wording that

an inspection. OSHA standards apply to any employer, defined as a "person engaged in a business affecting commerce who has employees," including religious groups to the extent that they employ workers for secular purposes. They do not apply to employees of federal or state governments. OSHA standards also do not apply to:

✳ Self-employed persons;
✳ Farms at which only immediate members of the farm employer's family are employed; and
✳ Working conditions regulated by other federal agencies under other federal statutes.

We can help you ensure your workplace meets applicable OSHA standards; please contact us for information.

prohibit a worker who is claiming workers' compensation benefits from receiving more than his/her pre-disability pay.

Short-term disability: Ideally, your organization's short-term disability benefits should kick in after a worker exhausts any available paid sick leave to prevent overlapping benefits.

Auto insurance: Personal auto policies often contain personal injury protection (PIP). In most states this coverage is optional, but some states require it. Also known as no-fault coverage, PIP pays for the insured's medical bills, loss of income and other costs related to an auto accident, regardless of who is at fault. Some states allow an insured to claim PIP benefits even if workers' compensation covers the claim. If you have workers in these states, you might be able to deduct PIP benefits from workers' compensation benefits. Your workers' compensation insurer's claims department will know the applicable laws.

Other Sources of Income for Injured Workers

Lawsuits: Workers' compensation law does not allow workers to sue their employers for workplace injuries. However, they can sue a third party (someone besides the employer or a co-worker) who causes or contributes to their injury—for example, the manufacturer

of a defective piece of equipment that causes injury.

Unlike the workers' compensation system, the tort system allows an injured person who prevails in a lawsuit to receive compensation for pain and suffering, property damage, loss of monetary support, loss of consortium, disfigurement and sometimes punitive damages, in addition to lost time.

When an employee collects tort damages or other settlements in addition to workers' compensation payments, the employer's insurer or the employer has the right to "subrogate," or claim a credit against any settlement or recovery received. Subrogation prevents an injured worker from collecting for the same injury twice; it also helps lower workers' compensation costs.

Other employment: We've all heard the stories of employees collecting workers' compensation disability benefits who get caught working under the table in physically demanding jobs. This sort of behavior goes beyond double dipping and constitutes fraud. If you suspect workers' compensation fraud, contact your insurer's fraud department.

We can help design benefits under workers' compensation and other programs to encourage, rather than discourage, injured employees to return to work. Please contact us for more information. ■

Romance in the Office

Spring is in the air, and so is love — even in the office. In a CareerBuilder poll released in 2013, 39 percent of workers said they have dated a co-worker at least once over the course of their career; 30 percent of those who have dated a co-worker said their office romance led them to the altar. It's the ones that don't that more likely cause problems for employers.

A soured relationship can lead to claims of sexual harassment, particularly when it involves co-workers on different rungs of the corporate ladder. Sexual harassment in the office, pervasive a generation or two ago, has become less acceptable due to changing social norms and more employer awareness and training. However, that does not mean it is not a problem. A generation ago, the victim of sexual harassment probably would have quit her job. Now, she (or he) can sue.

In 2011, the last year for which complete figures are available, the U.S. Equal Economic Opportunity Commission (EEOC) reported that it received 11,364 sexual harassment complaints. Of these, 10.9 percent came to a settlement, 9.1 percent were withdrawn "with benefits," and 26.1 percent were resolved "with merit." Complainants won $52.3 million in monetary benefits, which does not include monetary benefits obtained through litigation.

In addition to the cost of settlements and litigation, employers facing a sexual harassment claim can suffer a hit to their reputation and staff morale. As the EEOC says, "Prevention is the best tool to eliminate sexual harassment in the workplace."

What Exactly Is Sexual Harassment?

The EEOC defines two types of sexual harassment: quid pro quo harassment and "hostile environment" harassment. In quid pro quo harassment, someone in power exchanges something

(such as a raise or promotion) for sexual favors. This type of harassment is usually initiated by those in supervisory positions.

A "hostile work environment" can occur whenever unwelcome sexual conduct creates an environment that employees view as hostile or intimidating. Such conduct can include making unwelcome sexual advances or sexually offensive remarks, displaying sexually explicit pictures, or making crude jokes or obscene gestures.

Affairs between co-workers can sometimes lead to problems with other workers. Some courts have recognized "sexual favoritism" as sexual harassment because it creates a "hostile work environment" for the other workers.

What Action Steps Can Employers Take?

Until the 1970s and early 1980s, many companies banned employee dating outright. As of 2005, only 18 percent of human resource managers surveyed by the Society of Human Resource Management said their employer had written policies on workplace romances. Of those that did have written policies, 20 percent permitted romances among co-workers, 48 percent "permitted but discouraged" them, 31 percent forbade them, and 2 percent did not know.

Some companies take a proactive approach to dealing with interoffice romances. When an interoffice romance comes to light, some have the parties involved sign a "love contract," which stipulates that the relationship was entered into willingly and that, if it ends badly, neither party will hold the employer liable for sexual harassment.

If the relationship involves a subordinate and supervisor, some companies provide the parties a notice stating sexual harassment is a form of sex discrimination that violates Title VII of the Civil Rights Act of 1964. Other companies prohibit these relationships outright and require the transfer of one of the employees to another department when a relationship occurs or becomes public.

However, employers should be careful not to violate employees' privacy. Even if you suspect an interoffice romance, do not overstep. You probably will not want to make inquiries unless the relationship is between a supervisor and subordinate, has triggered complaints from one of the parties or other employees, or has affected work performance.

If you're interested in developing a written workplace romance policy, see the website of the Society for Human Resource Management (SHRM)'s template at www.shrm.org/TemplatesTools/Samples/Policies/Pages/CMS_006713.aspx. If you have concerns over a particular situation, though, you might want to consult an attorney experienced in employment matters. Your commercial general liability policy does not cover sexual harassment and other employment-related lawsuits. For information on protecting your company from the financial risk of sexual harassment and other employment-related lawsuits with employment practices liability insurance, please contact us. ◼

10 Cyber Security Tips for Small Business

Target and its customers are continuing to feel the repercussions of a massive data breach, where hackers gained access to data from some 40 million debit and credit cards of Target shoppers during the holiday season. The lesson for other businesses is clear: If the country's third-largest retailer, with its resources and sophisticated systems, can have a data breach, any business can.

The Federal Communications Commission offers the following tips to help small businesses protect their networks and prevent security breaches.

1 **Train employees in security principles.**
    Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.
2 **Protect information, computers and networks from cyber attacks.**

Keep clean machines: having the latest security software, web browser and operating system are the best defenses against viruses, malware and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

3 Provide firewall security for your Internet connection.

A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.

4 Create a mobile device action plan.

Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password-protect their devices, encrypt their data and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

5 Make backup copies of important business data and information.

Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.

6 Control physical access to your computers and create user accounts for each employee.

Prevent access or use of business computers by unauthorized individuals. Laptops and tablets can be particularly easy targets for theft or can be lost, so lock

them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

7 Secure your Wi-Fi networks.

If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password-protect access to the router.

8 Employ best practices on payment cards.

Work with banks or processors to ensure they use the most trusted and validated tools and anti-fraud services. You may also have additional security obligations pursuant to agreements with your bank or processor. Isolate payment systems from other, less secure programs and don't use the same computer to process payments and surf the Internet.

9 Limit employee access to data and information; limit authority to install software.

Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.

10 Have password protection and authentication procedures.

Require employees to use unique passwords and change passwords every three months. Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that

handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.

Standard business property and liability policies do not cover data losses. To ensure you have coverage when you want it, you need a specialized cyberinsurance policy. Look for a policy that provides coverage for both remediation and fines and penalties.

One of the most common reasons smaller businesses fail to buy cyber-insurance is that they think they are too small for hackers to bother. However, as larger companies do more to secure their technology systems (the Target incident notwithstanding), less-secure small businesses are becoming easier targets for cybercriminals. For more information on these nonstandard policies, please contact us. ■

Work Hardening: Another Tool in Your Return-to-Work Kit

Sometimes, an injured worker might have reached maximum medical improvement but be unable to return to work due to loss of strength or a partial disability. Work hardening programs can help these workers transition from disability to productive employment.

The work hardening process consists of:

✳ **Referring.** Typically, a treating physician will refer an injured worker to an occupational or physical therapist for work hardening. A medical exam will provide the therapist with information on the worker's medical condition and any physical restrictions.

✳ **Evaluating.** The therapist will evaluate the returning worker's baseline strength and conditioning levels, using treadmills, ergometers, free weights, etc.

✳ **Analyzing.** The therapist analyzes the physical demands of the job and its ergonomic environment.

✳ **Planning.** Using this information, the therapist develops a comprehensive plan to return the employee to his/her former job. Specific tasks include the following:

✳ **Strengthening.** The therapist develops an individualized program of real or simulated work tasks. These progressively more difficult tasks help an injured worker regain strength and retrain unused muscles.

✳ **Modifying.** Where necessary, the therapist can recommend workplace modifications that can help injured workers with disabilities perform the critical tasks of the job. These might range from rearranging the workstation to specifying customized adaptive equipment.

✳ **Educating.** A good work hardening program will help train an injured worker in preventive self-care. If poor body mechanics, lack of fitness or other worker characteristics led to or contributed to the injury, the therapist should provide training on proper body mechanics, such as proper lifting techniques, and other ergonomic safety suggestions.

✳ **Coping.** Where necessary, a work hardening program can include measures to help a worker cope with any remaining symptoms from the injury, such as pain.

✳ **Discharging.** The therapist will monitor the worker's progress, recommending return to work when he/she has reached predetermined strength and work fitness goals. Programs typically last three to four weeks.

Many studies have found work hardening to be an effective, albeit costly, method of returning injured workers to work. For more information on this and other claim management strategies, please contact us. ■

Managing Risk ♟♚

SmartsPro
MARKETING