



<http://www.coupagency.com>

49 Broadway
Milton, PA 17847
570-742-8736
800-ERA-COUP
FAX: 570-742-3711

110 Market Street
Lewisburg, PA 17837
570-524-9908
FAX: 570-524-5772



For more information or a quotation call 800-372-2687

Risk Review *Keeping you informed on Business Insurance issues*

Volume 16, No. 1

Workers Compensation: Keeping an Eye on Employees

Generally, workers compensation law substitutes the common-law rights of a covered employee, such as the right to sue an employer, with a legal remedy that requires the employer to pay benefits according to an applicable state statute.

State workers compensation statutes cover most forms of employment within that state. However, laws differ among states, and they may not be mandatory in every state. In addition, federal statutes limit coverage to federal employees and workers employed in some significant aspect of interstate commerce.

While some state compensation laws prohibit lawsuits brought against employers by their employees, exceptions may arise if recovery based on negligence results in a more suitable remedy than the applicable workers compensation statute. Two common exceptions are **intentional harm**, i.e., injuries arising from safety violations, and **bad faith**, i.e., undue harassment of an employee during the claims process.

Who Benefits?

Basically, workers compensation is the legal recognition by an employer that an employee has sustained a work-related injury. This acknowledgement may then obligate the employer to pay for medical

expenses, temporary and permanent disability benefits, rehabilitation benefits, and survivor benefits in the event of death.

Under a common-law remedy, the injured worker may experience delays and litigation expenses, and he or she may not receive compensation until a court rules or the parties reach an agreement outside the legal system. Under a typical workers compensation statute, however, the employee is guaranteed workers compensation benefits on a timely basis. In turn, the employer is protected from all potential financial losses associated with the related injuries, which could be substantial if employer negligence were proven in a court of law. The employer may control these potential losses through insurance premiums for workers compensation coverage.

For Better or Worse

While both parties have relinquished rights under the modern system of workers compensation—the employee's right to a common-law remedy and the employer's right of due process—the benefits produced under state statutes generally provide for the welfare of both groups. Consider speaking with one of our insurance professionals, who can help evaluate potential risks and structure an appropriate insurance program to help prevent losses to your business.

Find the Right Insurance Program for Your Business

The purpose of having a **business insurance and risk management program** in place is to provide sufficient protection for your business in the event of a loss. The cost of implementing a loss prevention program may, at first, appear to be an unnecessary expense. However, a successful program can work toward alleviating the damaging effects of loss. It may also help save indirect costs and keep insurance premiums at their lowest. Maintaining documentary evidence prior to a loss is important to sustain claimed values if your business should suffer a loss.

When determining the best program for your business, consider the following: What are the potential losses that your business could suffer? What effect could those losses have on your business? How can you reduce your risk exposure? What is the best blend of risk management, business insurance, and self-insurance for you and your business? Our insurance professionals are trained to assist you with this evaluation; give us a call.

Protecting Customers from Identity Theft

Identity theft can have devastating financial and psychological consequences for individuals whose personal information is stolen. When thieves make purchases, empty bank accounts, or take out loans under other people's names, it can take months, or even years, for victims to restore their credit records.

Identity theft can also have a catastrophic effect on businesses that fail to adequately protect confidential data. "Losing" a customer's data can result in litigation or fines, and it may damage a company's reputation irreparably if a data breach is made public. Smaller companies, in particular, are at risk of being targeted by identity thieves as larger companies become more adept at warding off attacks by hackers and other thieves.

Here are some of the precautions you, as a business owner, can take to reduce the risk of sensitive customer data falling into the wrong hands:

- Minimize the amount and types of information collected. The theft of Social Security numbers can be particularly damaging to individuals, so companies should use other means of identifying customers whenever possible. Even less sensitive types of information, such as phone numbers and birth dates, can be attractive to thieves.
- Conduct all e-commerce transactions through authentication systems with several layers of security designed to verify that the user who accesses an account or provides information is the legitimate owner of that information.
- Draft a privacy policy and train employees on these procedures. Firms should have in place a privacy policy with rules on the handling of customer data, and all employees with access to sensitive data should be instructed in these rules.
- Restrict employee access to data. Employees should be authorized to view or handle data on a "need-to-know" basis. There are software programs available that allow you to monitor who is accessing data at any given point in time; store this information should an audit become necessary later. Access to the company's databases should be withdrawn immediately when an employee leaves the company.
- Remind employees that phone conversations can be overheard and computer

screens can be viewed by unauthorized individuals. Employees should take care when discussing confidential information and lock their computers when they are away from their desks.

- Shield your computer network with firewalls designed to create a protective barrier between your company's network and the Internet. Available as either software or hardware, firewalls can stop potential hackers from gaining access to confidential information stored in your system.
 - Use encryption when exchanging sensitive information with customers via a website or e-mail, and encrypt confidential customer data stored on servers and backup systems. Encryption software scrambles data during transit over the Internet, making it difficult for hackers to intercept and steal customers' information.
 - Install antivirus and anti-spyware software packages on all company computers. These programs should include automatic updates and should never be disabled.
 - Store information in the most secure location possible, and properly dispose of old records. If it is not necessary to keep customer information online, it is safer to store it offline in file cabinets under lock and key. Hard copies of records containing sensitive information should be shredded when no longer needed.
 - Protect hardware from tampering or theft. Thieves can tap into sensitive data stored on servers or the hard drives of computers and notebooks if they find or steal the equipment. Businesses should run hard-drive shredding software before disposing of old computer equipment.
 - Include as little personal information as possible in written correspondence to customers, as thieves can steal Social Security and account numbers by intercepting mail.
- Should a data breach nonetheless occur, it is essential to take prompt action. The compromised accounts should be suspended immediately, and the systems containing the data should be shut down to prevent additional theft. Notify the police and the FBI of the breach, as well as any customers who might be affected. Your company's security systems should be thoroughly analyzed to establish how the breach occurred, and steps should be taken to prevent future losses.

For Your Information

Promoting Health and Safety

According to a survey conducted by human resources consultancy Watson Wyatt and the National Business Group on Health, 85% of employers provide tools that encourage safety and wellness, 82% promote emotional health, 63% educate employees on safety at work, and 52% involve senior management in promoting health and productivity. While only 29% of respondents indicated their organizations currently connect wellness programs to broader company goals, 55% said they intend to forge this link by 2009.

Print and Online Ads

Small businesses consider Yellow Pages print advertising to be most effective in generating sales leads, but also recognize the Internet as a growing media source, according to a survey sponsored by AT&T. Results revealed that 63% of small businesses currently advertise in a printed Yellow Pages directory, the most commonly cited form of advertising by almost a 2-1 margin. In addition, around 23% currently advertise online, and two-thirds have their own website.

Changes in Health Benefits

According to a survey by the Employee Benefit Research Institute (EBRI), 63% of respondents with health care coverage experienced an increase in their insurance contributions over the past year, and 81% said that this has motivated them to take better care of themselves. Further, 54% of employees with coverage said they are not confident that they would be able to obtain insurance independently if their employer stopped offering a health plan.