FEBRUARY 2019

RISK Monitor

A Newsletter for Clients and Friends of Galloway Chandler McKinney Insurance

Computer Vision Syndrome, the New Safety Threat

COMPUTER VISION Syndrome, or CVS, is more common than carpal tunnel syndrome and other musculoskeletal disorders, according to *HR News*.

According to the American Optometric Association, CVS is a result of interaction with a computer display. Symptoms of CVS are eye strain and fatigue, dry eyes, headaches and neck and shoulder pain.

Computer terminal-related vision problems are at least as significant a health concern as the musculoskeletal disorders, such as carpal tunnel syndrome, that receive more attention.

In most cases, CVS is treatable – and modifications to the workplace and regular practices can help. VSP VisionCare, an eye-care insurance company, says that you can take simple steps to combat CVS among your workers.

TIPS FOR COMBATING EYE STRAIN AMONG YOUR STAFF

Keep blinking – It washes your eyes in naturally therapeutic tears.

Remember 20-20-20 – Every 20 minutes, spend 20 seconds looking at something 20 feet away, minimum.

Get the right light – Good lighting is healthy for your eyes. So, keep bright lighting overhead to a minimum.

Keep your desk lamp shining on your desk, not you. Try to keep window light off to the side, rather than in front or behind you. Use blinds and get a glare screen.

Position the computer screen to reduce reflections from windows or overhead lights.

Monitor your monitor – Keep it at least 20 inches from your eyes.

The center of the screen should be about 4 to 6 inches below your eyes.

Also, make sure it's big enough and with just the right brightness and contrast.

Adjust the screen so you look at it slightly downward and are about 24 to 28 inches away.

Adjust the screen settings to where they are comfortable – contract polarity, resolution, flicker, etc.

Wear those computer specs – Your doctor can prescribe a pair of glasses just for seeing the computer screen well.

If necessary, wear the appropriate corrective lenses while at the computer. ❖

Welcome to the Galloway Chandler McKinney Insurance Newsletter!

It is with great satisfaction that we bring this newsletter to you. In this issue and in coming months, we will discuss pertinent risk management topics which may affect your organization. We sincerely hope that you will find this newsletter informative and please do not hesitate to contact us should you have any questions or needs.

GCM

GALLOWAY-CHANDLER-McKINNEY INSURANCE

www.gcminsurance.com

OSHA Stays Serious About Temp Worker Safety

WHILE THE Trump administration has eased off a number of regulations and enforcement actions during the past two years, Fed-OSHA continues focusing on the safety of temporary workers as much as it did under the Obama presidency.

This puts the onus not only on the agencies that provide the temp workers, but also on the companies that contract with them for the workers.

As evidence of its continued focus on temp workers, OSHA recently released guidance on lockout/tagout training requirements for temporary workers. This was the third guidance document released in 2018 and the 10th in recent years that was specific to temp workers.

One reason OSHA is so keen on continuing to police employers that use temporary workers, as well as the staffing agencies that supply them, is that temp workers are often given some of the worst jobs and possibly fall through the safety training cracks.

OSHA launched the Temporary Worker Initiative in 2013. It generally considers the staffing agency and host employer to be joint employers for the sake of providing workers a safe workplace that meets all of OSHA's requirements, according to a memorandum by the agency's office in 2014 to its field officers.

That same memo included the agency's plans to publish more enforcement and compliance guidance, which it has released steadily since then.

OSHA TEMP WORKER GUIDANCE

- Injury and illness record-keeping requirements
- Noise exposure and hearing conservation
- Personal protective equipment
- Whistleblower protection rights
- Safety and health training
- Hazard communication
- Bloodborne pathogens
- Powered industrial truck training
- Respiratory protection
- Lockout/tagout

Joint responsibility

OSHA started the initiative due to concerns that some employers were using temporary workers as a way to avoid meeting obligations to comply with OSHA regulations and worker protection laws, and because temporary workers are more vulnerable to workplace safety and health hazards and retaliation than workers in traditional employment relationships.

With both the temp agency and the host employer responsible for workplace safety, there has to be a level of trust between the two. Temp agencies should come and do some type of assessment to ensure the employer meets OSHA standards, and the host employer has to provide a safe workplace.

Both host employers and staffing agencies have roles in complying with workplace health and safety requirements.

Each employer should consider the hazards it is in a position to prevent and correct, and in a position to comply with OSHA standards. For example: staffing agencies might provide general safety and health training, and host employers provide specific training tailored to the particular workplace equipment/hazards.

KEYS TO SUCCESS

- Communication between the temp agency and the host is key to ensuring that the necessary protections are provided.
- Staffing agencies have a duty to inquire into the conditions of their workers' assigned workplaces. They must ensure that they are sending workers to a safe workplace.
- Ignorance of hazards is not an excuse.
- Staffing agencies need not become experts on specific workplace hazards, but they should determine what conditions exist at the host employer, what hazards may be encountered, and how best to ensure protection for the temporary workers.
- The staffing agency has the duty to inquire and verify that the host has fulfilled its responsibilities for a safe workplace.
- Host employers must treat temporary workers like any other workers in terms of training and safety and health protections.

For a look at all 10 of the guidance documents OSHA has issued in the last few years, visit the agency's temp worker page. ❖

Estate Planning: Passing on the Family Business

A SUCCESSFUL family business is a cornerstone of many families' wealth. But passing the business along to the next generation takes substantial planning and preparation.

A recent Pricewaterhouse Coopers report found that while just over half of family-owned business executives wanted to pass on their businesses to children, just 27% of these companies had a robust, actionable succession plan in place.

Here are some important things to keep in mind:

Choose the appropriate entity

You can't pass on an existing family business as a sole proprietorship or general partnership. You can pass on the assets, but not the business itself. Also, you can't pass S-corporation shares to a non-resident alien.

Involve family in business succession discussions

Get family input years ahead of time, and involve them when discussing succession planning. Sometimes family members may not want to go into the family business.

Knowing this in advance can help you make a solid plan.

Have a will and buy-sell agreement in place

All shareholders should have a will precisely defining what happens to their share of the business upon their death. Without a will, a deceased owner's interest would automatically go to his or her spouse, children or other next of kin according to most states' default intestate laws.

A will and a buy-sell agreement ensure that control of the company will remain with the people committed to the business.

A life insurance policy on each shareholder, with the company or with the other owners as beneficiaries, may be a good way to ensure that there will be enough cash available to buy out surviving spouses or other heirs of any deceased shareholder.

Consider passing on ownership, not management

Sometimes adult children of entrepreneurs may not want to manage the day-to-day business. But they could be excellent as directors and shareholders. In this case, work on recruiting and developing a manager to run the firm as an employee.

If this isn't practical, it may be best to explore selling the business outright.

Make equitable arrangements for other children

If you have multiple children, chances are at least one of them will not want to take over the family business, or will be unable to do so for any number of reasons. Possible solutions:

- Start amassing assets outside of the business.
- Own life insurance sufficient to equalize the inheritances.
- Divide the business's ownership into voting and non-voting shares, in order to give the most capable or involved child operational control without disinheriting the others

Provide for founder's retirement income security

The business should provide an income for the founder and their spouses for as long as they live. Possible techniques include:

- **Purchase.** The founder's children pay the founder outright in cash for his or her shares, either in a lump sum or installments.
- **Preferred stock.** Convert the founder's interest from common stock to preferred stock. The founder doesn't get to vote shares anymore, and no longer controls the company. But preferred stock dividends get paid first.

Nobody can take any dividends out of the business unless the preferred stock dividend is paid.

Upon the founder's death, the preferred stock goes to the surviving spouse, and then gets passed on according to the last will and testament. ❖

THE TAKEAWAY

Don't try to wing this process! Family-business succession planning is a long process, and you'll need the help of attorneys, tax professionals, insurance professionals and business valuation experts along the way.

IF YOU HAVE QUESTIONS, CALL US!

As Data Breaches Grow, Few Small Firms Act

AS THE number of data breaches involving smaller businesses continues to grow, a survey by The Hartford finds 85% of small business owners believe a potential breach of their own data is unlikely, and many are not implementing simple security measures to help protect their customer or employee data.

"Most of the business owners surveyed believe they are not at risk, when in fact smaller businesses are increasingly being targeted," said Lynn LaGram, assistant vice president of small commercial underwriting at The Hartford. "It is important for business owners to take proactive measures to protect data and minimize the likelihood of a breach."

More than a third said they have a more negative opinion of companies that have recently experienced a breach, based on the companies' handling of the breach.

About a third of business owners said they would have difficulty complying with laws requiring that they notify the affected parties if a breach were to occur, and nearly half acknowledge it would be impossible for a small business to completely safeguard customer, patient or employee data.

DATA PROTECTION PRACTICES

The Hartford asked the business owners how they protect their data:

- Lock and secure sensitive customer, patient or employee data (48%)
- Restrict employee access to sensitive data (79%)
- Shred and securely dispose of customer, patient or employee data (53%)
- Use password protection and data encryption (48%)
- Have a privacy policy (44%)
- Update systems and software on a regular basis (47%)
- Use firewalls to control access and lock out hackers (48%)
- Ensure that remote access to their company's network is secure (41%)

Data breach coverage

Besides these methods, businesses of any size that store sensitive employee or customer information should also consider purchasing insurance to help them respond to and recover quickly from a breach.

Data breach coverage is typically issued as an endorsement to your company's business owners' policy and will generally provide coverage for expenses and legal liability resulting from a breach.

Some carriers also offer access to services to help their insureds comply with data breach notification laws.

Companies that store sensitive client or patient data, such as those in health care, financial or professional services, and restaurants and retailers with the large volume of credit-card information they process, should consider this coverage. ❖

WHAT INSURANCE COVERS

- First party coverage for response expenses, including legal and forensic services, notification expenses, crisis management and good-faith advertising expenses;
- Third party coverage for defense and liability, including defense costs, civil awards, and settlements or judgments that an insured is legally obligated to pay; and
- Consultation, including help with breach notifications.

GCM
GALLOWAY-CHANDLER-McKINNEY INSURANCE
www.gcminsurance.com
RISKMonitor