News You Can Use

February 2024
Volume 12
Issue 2

HEFFERNAN INSURANCE BROKERS
Because You're Different

Worker Classification

DOL Issues Final Independent Contractor Rule

THE U.S. Department of Labor in January 2024 finalized a new federal rule that will make it more difficult for employers to classify workers as independent contractors. The final rule formally rescinds the independent contractor rule issued by the DOL during the Trump administration a few years ago and provides a different interpretation of how the key test of employment, called the "economic realities test," should be applied.

But for employers it is likely to sow confusion and may result in individuals being improperly designated as employees when they are, in fact, operating as independent contractors.

Companies who hire contractors that work exclusively for them will have the hardest time trying to continue classifying them as independent contractors. Here are the proposed changes you may want to pay attention to in case your firm uses outside contractors.

The final rule

The new rule allows an employer to classify someone as an independent contractor if, "as a matter of economic reality," that person is in business for themselves. What "economic reality" is depends on the answers to a six-pronged test:

(Note: One answer by itself does not make a person an independent contractor.)

Can the worker increase their pay only by working more hours or producing more? If so, this might make the person an employee. Conversely, can they do so by negotiating pay, selecting projects, marketing their service or cutting expenses? That would tend to make them an independent contractor.

Does the employer purchase most of the worker's tools and equipment? This might make the person an employee. On the other hand, if their investments are for purposes like expanding the types and amounts of work they can do or cutting expenses, that might tend to make them an independent contractor.

Under the rule, when comparing investments made by the worker and potential employer, the analysis should focus on the types of investments made by each and not focus exclusively on the relative size of the investments.

Does the employment relationship have a definite end date? If so, this implies that they're an independent contractor. Otherwise, they might be an employee.

How does the employer control the worker, and how much? The worker may be an employee if the employer:

- Sets their schedule
- Supervises the work
- Explicitly limits their ability to work for others
- Can discipline the individual
- Monitors their activity.

See 'Revisit' on page 2

CONTACT US

If you have any questions regarding your coverage or our products, please call us at one of our offices:

Walnut Creek
San Francisco
Petaluma
San Jose
San Mateo
Truckee
Bakersfield
Woodland Hills
London
Cypress
Los Angeles
Irvine
Phoenix
Portland
Seattle
St. Louis
Philadelphia

Phone: 800-234-6787
CA License No.: 0564249

Workplace Safety

New OSHA Electronic Reporting Rule Takes Effect

A NEW RULE by the Department of Labor requires firms with 100 or more employees in certain industries to electronically submit their OSHA Form 300 and 301 logs, starting in 2024. These are in addition to submission of Form 300A (Summary of Work-Related Injuries and Illnesses).

The new rule applies to businesses in 104 high-hazard industries that include the agricultural, food production, manufacturing, retail, wholesale, transportation and medical sectors.

All employers that are subject to OSHA regulations are required to annually submit to OSHA Form 300 (Log of Work-Related Injuries and Illnesses) and Form 301 (Injury and Illness Incident Report), and their Form 300A.

The new rule leaves in place existing regulations requiring:

- Businesses with 20 to 249 workers in certain high-hazard industries to electronically submit information from their Forms 300A once per year.
- All employers with 250 or more workers to electronically submit information from their Forms 300A once per year.

The final day to submit the above electronic files is March 2, 2024. You can find a full list of the affected 104 industries here. ❖

IT'S TIME TO POST YOUR OSHA FORM 300A

Employers with 10 or more employees must post their completed OSHA Form 300A by Feb. 1 and keep it posted in their workplace until April 30.

The form must be posted where the company usually posts other staff notices, like minimum wage and worker rights posters. The Annual Summary (Form 300A) requires the following information from the Form 300 Log:

- The total number of non-first-aid injury and illness cases.
- The total number of cases with days away from work and cases with job transfer or restriction, and total number of other recordable cases.
- The total number of days from all injuries, including days away from work and job transfer restrictions.
- The number of injury/illness cases, including skin disorders, respiratory conditions, poisoning and hearing loss.

Continued from page 1

Revisit Your Practices If You Use Independent Contractors

Is the person's work integral to the employer's business? The more integral the work is, the more likely the person is to be an employee. The less integral it is, the more likely they are to be an independent contractor.

Does the worker use specialized skills developed outside the employment? If the worker doesn't use specialized skills or depends on the employer for training, they are more likely to be an employee. If the person brings those skills to work and does not rely on the employer for training, they are more likely an independent contractor.

The takeaway

If your firm uses independent contractors as a normal course of business, you will need to revisit your practices and determine if the new rule changes your relationship with them. It may be wise to consult legal counsel.

Finally, business organizations have already indicated they will challenge the rule-making in court. And some Senate Republicans have said they will seek to repeal the rule via the Congressional Review Act.

For now, however, the new rule is codified and applicable. It takes effect on March 11, 2024. ❖

Produced by Risk Media Solutions on behalf of Heffernan Insurance Brokers. This newsletter is not intended to provide legal advice, but rather perspective on recent regulatory issues, trends and standards affecting insurance, workplace safety, risk management and employee benefits. Please consult your broker or legal counsel for further information on the topics covered herein. Copyright 2024 all rights reserved.

Protecting Your Data

The 2024 Cyber-Security Threat Landscape

THE CYBER-security landscape changes constantly. For employers, it's important to stay on top of these threats so that they can ensure that their security protocols and internal procedures are up to the task of beating them back.

Recent reports from cloud-computing provider Google Cloud and cyber-security vendor Netwrix forecast several trends, including:

- **Tighter cyber insurance requirements.** Insurers already insist that their policyholders implement employee security training, multi-factor authentication and security patch management. Netwrix predicts that in 2024 carriers will also require user identity and access management practices.
- **Artificial intelligence will have mixed effects.** Google Cloud says criminals will use AI to make phishing attacks and information-theft attempts more convincing. However, it will also make event response and analysis faster.
- **Theft of encrypted data will become more frequent**. Netwrix says criminals will bet on future improvements in technology that will permit them to eventually unlock encrypted data that is unintelligible today.
- **Criminals will seek out and exploit 'zero-day vulnerabilities.'** These are security holes in software that are unknown to the manufacturer or vendor when it is released. Criminals will look for these weaknesses to infiltrate systems.
- **AI will make criminals convincingly multilingual.** Netwrix expects criminals to use AI to write e-mails in languages other than English and with better grammar. This will make phishing e-mails more difficult for even wary users to spot.
- **Security fatigue will become a greater problem.** Experts and organizations warn users often about cyber-security risks and require frequent training. However, the constant warnings and admonitions about passwords may wear them out.

Users accessing systems remotely may have to enter as many as five or six passwords before they even begin working. Security fatigue can cause user errors that security is supposed to prevent.

WHAT TO DO

These new challenges can seem overwhelming, but there are things individuals and businesses can do to face them:

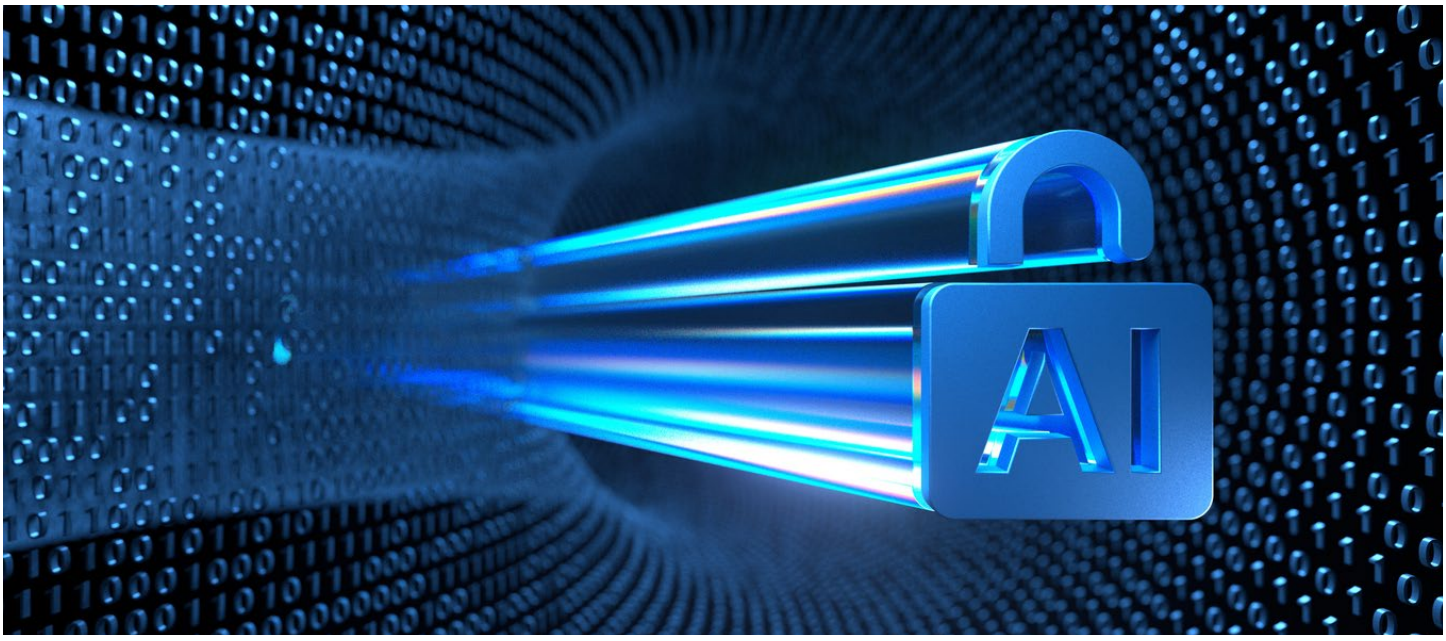
- Regularly assess cyber-security risks and implement improved mitigation methods to address them.
- Make encryption one facet of data protection, not the only one. Invest in incident detection technologies and create a written plan for incident response.
- Recognize that stolen encrypted data may not be used immediately. Monitor the internet for future use of the data.
- Update phishing training for users so they will be more suspicious of even convincing e-mails.
- Similarly, train non-English speakers on the potential for phishing e-mails in their languages.
- Require users to have unique strong passwords that they must change every three months or less.
- Limit and control the use of system administrator access.
- Tailor awareness training to the needs of specific user groups to avoid overwhelming all users with security information they might not use.

The takeaway

Besides having in place cyber-security protocols, you should also have a robust cyber insurance policy. ❖

Protect Your Business's Data and IP

ASK US ABOUT CYBER INSURANCE



Risk Management

The Perils of Not Keeping Up Your Commercial Property

IF YOU OWN a commercial property or lease a building, you not only have to be concerned about risks that cause property damage, but also the risk of injury to visitors, customers and tenants.

It's your responsibility to keep your property free of hazards that can result in injury or worse. If you fail to live up to your responsibility, you risk being sued by the injured party.

Commercial premises liability claims can involve a wide range of situations, including:

Slip, trip and fall accidents – A slip and fall may have occurred due to wet or damaged floors. Trips and falls may occur due to obstructions in walkways and poor lighting during evening hours.

Property defects – If you fail to keep up the property or conduct regular maintenance, hazards can easily develop. When hazards and property defects arise, it's your responsibility to address them as soon as possible. And if it will take a while to make the repairs, you need to alert visitors, customers and tenants about the danger, like cordoning off an area and erecting visible signs warning of the hazard.

Negligent security – If your facility is located in an area with a higher than average level of criminal activity and break-ins, you are also expected to keep the premises and everybody visiting the site safe.

Poor lighting, a lack of security personnel and systems, and of other safety measures, can all lead to a negligent security claim.

Risks of inadequate lighting

There are three ways that inadequate lighting at a commercial property can contribute to a claim against your organization:

Making a safe area unsafe – Poor lighting can conceal conditions that would not be considered a hazard under normal lighting as they would be visible. Inadequate lighting makes it harder to see curbs, inclines in walkways, steps, borders for planters and other decorations.

Masking existing hazards – Inadequate lighting can be especially dangerous when it serves to conceal the presence of hazardous defects already existing on a property. For example, if a foreign substance has been spilled on the floor, while that would be considered a hazardous condition even when fully illuminated, it becomes doubly hazardous when obscured by darkness.

Creating a magnet for crime – Poor lighting can give cover and concealment to criminals intent on mugging or harming individuals at your property in the evenings. If you create conditions for a mugger to sneak up on someone in your dim parking lot or near the entrance to a poorly lit building, they could sue you for negligence.

How insurance can help

Commercial general liability insurance is an essential part of every business owner's insurance portfolio. It protects you and your business from claims of injury, property damage and negligence related to your business activities.

One of the most essential parts of the policy is premises liability coverage. This portion offers bodily injury and property damage coverage related to the ownership or maintenance of business premises.

Every business owner has some type of premises liability exposure. Any injury on your business premises, no matter how minor, can result in a lawsuit.

The costs associated with defending yourself and paying damages can be devastating for your business. Premises liability coverage gives you — and your guests — the protection you need.

If you are leasing space in a commercial building, your liability typically ends at the front door to your office and anything beyond that is the responsibility of the property owner. If you own and occupy a building, the entire property is your responsibility.

If you want more information on this type of insurance or want to evaluate your current coverage, give us a call. ❖