VanBeurden
INSURANCE SERVICES, INC.
Since 1934

A full-service agency with a passion for protecting you, your family, and your business.

NEWSBLAST
July 2024 | Volume 2 | Issue 3

Workplace Safety

Indoor Heat Illness Rules Coming Soon

THE CAL/OSHA Standards Board has voted to approve new heat illness prevention regulations that will require some workplaces to make significant adjustments to their operations in order to comply, possibly starting later this summer.

The indoor heat illness prevention standard applies to most indoor workplaces where the temperatures reach at least 82 degrees. According to Cal/OSHA, that includes facilites like warehouses, manufacturing and production facilities, greenhouses, wholesale and retail distribution centers, restaurant kitchens and dry cleaners.

The new standard is expected to take effect in August.

The rules

Applicable employers will need to create and maintain a written indoor heat illness prevention plan that includes the following:

82-degree trigger – When temperatures indoors reach this level, employers must:

- Have and maintain one or more cool-down areas when employees are present, which must be kept at a temperature below 82 degrees.
- Allow and encourage staff to take preventive cool-down rests in a cool-down area when they feel the need. They should be monitored for signs of heat illness during rests.
- Provide drinking water near the areas employees are working.
- Observe all employees during heatwaves when a workplace has no measures for controlling the effects of outdoor heat on indoor temperatures.

87-degree trigger – When the temperature exceeds 87 degrees, employers must measure the temperature and heat index, and identify all other environmental risk factors for heat illness.

Firms must keep records of the temperature/heat index.

They must also implement control measures such as:

- Using air conditioners, swamp coolers, ventilation or other measures to reduce the air temperature (engineering controls);
- Adjusting work procedures, practices or schedules to minimize exposure to heat, such as changing shifts to start earlier and avoid the hottest parts of the day (administrative controls); or
- Using personal heat-protective equipment, such as water- or air-cooled garments or heat-reflective clothing.

Employers with affected workplaces must also observe new employees for 14 days when working under these conditions.

Emergency response – Employers must develop emergency response procedures, which must include:

- An effective communication system to allow workers to contact a supervisor or emergency services.

See 'Employers' on page 2

VanBeurden
INSURANCE SERVICES, INC.
Since 1934

Kingsburg office
1600 Draper Street
Kingsburg, CA 93631-1911
(559) 897-2975

Woodland office
283 Main Street, Suite 100
Woodland, CA 95695
(530) 661-0666

Los Osos office
1330 Van Beurden Drive Suite #201
Los Osos, CA 93402
(805) 528-1484

www.**vanbeurden**.com
Ca. License No. 0376731

Why You Need Employment Practices Liability Coverage

EVERY EMPLOYER, no matter how small, faces the specter of being sued by a past, present or prospective employee at some time.

In fact, such employment practices claims are widespread — so much so that most businesses are more likely to have an employment practices liability claim than a general liability or property loss claim.

Nearly three-quarters of all litigation against corporations today involves employment disputes, which can be extremely costly. The cost associated with an employment practices claim can be significant.

The cost of employee lawsuits against employers is increasing and the Equal Employment Opportunity Commission has been busy enforcing discrimination and harassment complaints, including a collecting a record-breaking $665 million in recoveries in fiscal 2023, up 30% from 2022.Furthermore, the commission reported having one of the most litigious years in recent memory, with 142 new lawsuits filed, marking a 50% increase from 2022.

With this surge in activity, employment practices liability insurance is crucial for any employer. The risks of being sued by an employee for discrimination or harassment have increased substantially.

What EPLI Covers

- Defense costs (court fees, attorney fees and related costs).
- Payment of settlements and/or judgments up to the policy's limits.
- Any fines or penalties levied by government agencies.

EPLI policies cover business owners as well as directors, officers and managers. Some policies also cover employees.

Types of action covered include:

- Discrimination based on gender, race, national origin, religion, disability or sexual orientation
- Sexual harassment or other unlawful harassment in the workplace
- Wrongful termination
- Failure to employ or promote
- Retaliation
- Misrepresentation about work and employment
- Failure to adopt adequate workplace or employment policies and procedures
- Employment-related defamation or invasion of privacy
- Negligent evaluation of an employee
- Wrongful discipline of an employee
- Employment-related infliction of emotional distress.

Costs

EPLI claims can be extremely expensive. The average cost of a discrimination claim is $125,000, and 25% of judgments exceed $500,000.

Most businesses are wise to have at least $1 million in coverage. However, higher coverage limits increase your premium cost, so you want to balance your coverage needs and your budgetary concerns.

Call us if you want further information or need help in gauging your EPLI coverage needs. ❖

Continued from page 1

Employers Must Develop Emergency Response Procedures

- Steps for responding to signs and symptoms of heat illness, including first aid and providing emergency medical services.
- Emergency response procedures for severe heat illness.
- Monitoring employees exhibiting signs of heat illness, and not leaving them alone without offering them on-site first aid or medical services.

Training – Employees and supervisors will need to be trained on:

- Personal risk factors for heat illness.
- Their employer's procedures for complying with the regulations.
- The importance of frequent water consumption.

The takeaway

- The California Office of Administrative Law is reviewing the new regulations, and Cal/OSHA expects it will take effect sometime in August. ❖

Demand for Coverage Grows as Workers Try to Defray Costs

SALES OF voluntary group benefits grew at a record pace in 2023, as more employers expand their offerings and demand continues booming as employees seek out benefits that can defray costs, according to new research.

Premiums collected for employer-sponsored voluntary benefits jumped 6.7% during the year to an aggregate $9.3 billion, with all lines of coverage contributing to the growth, according to the Eastbridge Consulting Group's annual "U.S. Voluntary/Worksite Sales Report."

The findings underscore the value that employees place on these benefits, particularly in defraying health care-related costs.

Ancillary Benefit Sales Surge

- Group term life insurance premiums increased 10% from the 2022 level.
- Group universal life and whole life were up 9%.
- Critical illness insurance premiums were up 7%.
- Hospital indemnity premiums were 6% higher.
- Dental coverage was up 5%.
- Short-term disability coverage was up 4%.
- Accident insurance rose 4%.

Source: U.S. Voluntary/Worksite Sales Report 2023

The biggest driver: personal finances

One of the main drivers of this surge in employee uptake of voluntary benefits is that they can often defray expensive and sudden expenses.

With the increase of high-deductible health plans and the resulting potential high out-of-pocket expenses workers may face, they are gravitating towards products that can provide much-needed cash in case of an unexpected event. These include many of the benefits that have seen strong sales growth in the last few years:

Accident insurance – This coverage provides a lump-sum cash payment to an individual due to an event covered under the policy. The funds can be used as needed to help cover things like deductibles, out-of-pocket medical costs or everyday living expenses.

Critical illness insurance – This provides a lump-sum payment or monthly payments to help cover expenses if a policyholder is diagnosed with a serious illness covered by the policy. This type of insurance supplements their existing health insurance and is designed to help them focus on recovery instead of costs.

Hospital indemnity – Hospital indemnity insurance supplements existing health insurance coverage by helping pay expenses for hospital stays.

Depending on the plan, the insurance gives the policyholder cash payments to help pay for the added costs that may arise while they recover.

Other products that help policyholders save money include dental and vision insurance, pet insurance (in the face of massive increases in veterinary costs), income protection and telemedicine services.

The takeaway

There are a number of other voluntary benefits that employers can offer, but the above are the ones that directly can help your employees if medical bills hit unexpectedly.

Premiums for these various coverages are either paid by the employer, split between the employer and employee or solely paid by the worker. Arrangements will vary between employers. Premiums are often reasonable.

More importantly, these coverages offer peace of mind that in the event of an accident or illness, the related expenses won't break the bank. ❖

EMERGENCY COVERAGE: *Accident insurance can provide a valuable financial backstop for your workers.*

Business E-Mail Compromise Scams Top Threat

BUSINESS E-MAIL compromise scams are now the most common type of cyberattack businesses face, and all types of these attacks are showing no signs of letting up, according to a new report.

Nearly three out of every four businesses were targets of these attacks and 29% of those firms became victims of successful attacks, according to the report by Arctic Wolf, a cyber-security firm.

While this has become the most common type of attack, a number of other schemes like ransomware attacks and data breaches continue growing in number.

Any of these attacks can drain a company's finances and result in tricky legal and possibly reputational issues that take time and money time to resolve.

The trends

The main threats businesses face, according to the report, are:

Business e-mail compromise (BEC) – Seven in 10 organizations surveyed said they had been targeted by these types of scams.

Some examples of BEC attacks include impersonating company executives to request wire transfers, falsifying invoice payment details, and tricking employees into revealing sensitive information. These scams can result in significant financial losses for businesses.

CAUTION: For businesses that use cloud-based e-mail services like Office365, these attacks are hard to detect since they don't reside on company servers.

With many organizations moving to cloud-based e-mail services, these types of attacks can be difficult to identify with traditional security tools and may go undetected until they have successfully executed their objectives.

Data breaches – Nearly half (48%) of organizations surveyed reported that they'd found evidence of a breach in their systems. The authors said that does not mean that the other 52% didn't suffer a breach; it means they failed to find evidence of one.

Ransomware – Some 45% of organizations surveyed admitted to being the victim of a ransomware attack within the last 12 months. These attacks usually involve criminals gaining access to a company's systems by getting an employee to click on a malicious link, after which they lock down the system and demand a ransom to unlock it.

Increasingly, perpetrators are also stealing data and demanding a second ransom to give it back and not release the data to others.

What you can do

How to Protect Against BECs

- Register all domain names that are similar to the business's legitimate website and can be used for spoofing attacks.
- Create rules that flag e-mails received from unknown domains.
- Monitor and/or restrict the creation of new e-mail rules on your servers.
- Enable multi-factor authentication.
- Conduct BEC drills, similar to anti-phishing exercises.
- Companies that use Office 365 or other cloud-based e-mail services, should employ detection tools or services specifically designed to monitor for threats related to BEC scams.

To combat ransomware:

Regularly back up system. Verify your backups regularly. This way you can restore functions if hit by ransomware.

Store backups separately. In particular, store backups on a separate device that cannot be accessed from a network, such as on an external hard drive.

Train your staff. Train your staff in how to spot possible phishing e-mails that are designed to convince an employee to click on a malicious link that will release the ransomware. ❖