Provided by Risk Strategy Solutions

RISK
ADVISOR

July 2024

COMMERCIAL

Tips for Business to Prevent Carbon Monoxide Poisoning

Carbon monoxide (CO) is a colorless, tasteless and odorless poisonous gas that is a byproduct of the incomplete burning of carbon-containing material. It can quickly accumulate in areas where employees work, even if the space appears well-ventilated. Exposure to CO can cause serious health problems and even fatalities, so business owners must take steps to ensure their workplace is safe. In order to do so, it is necessary to recognize the signs of CO poisoning and implement measures to minimize CO risks.

Recognizing CO Poisoning

CO poisoning symptoms can vary by person, and some populations are more susceptible to it, including the elderly, young children, individuals with preexisting heart or long-term conditions, those who work at high altitudes, those with anemia or sickle cell anemia, and those with elevated CO blood levels (e.g., smokers). CO poisoning also poses special risks to pregnant workers and their unborn children.

Early signs of CO poisoning can be mistaken for other illnesses and often mimic the flu or other illnesses. Symptoms include headache, dizziness, weakness, nausea and chest pain. Prolonged or high levels of CO exposure may lead to confusion, vomiting, muscle weakness, collapse and loss of consciousness. Neurological symptoms, metabolic acidosis and cardiac issues may also occur. According to OSHA, CO poisoning can be reversed if caught in time. However, as inhaled CO displaces oxygen in the blood and leads to vital organs becoming oxygen-starved, acute poisoning may cause permanent damage to organs that require high oxygen levels, such as the brain and heart. Additionally, OSHA notes that significant reproductive risk is linked to CO exposure.

Tips to Minimize CO Risks

Considering the severity of CO hazards, business owners need to take steps to eliminate or reduce the potential for CO-related injuries or fatalities, including:

- **Follow applicable manufacturer instructions and building codes** to ensure proper installation of equipment, appliances or other machines that may produce CO.
- **Schedule regular professional inspections** of heating systems, chimneys, flues and other equipment that could produce CO. Air in spaces where the gas may be should also be consistently tested for the presence of CO.
- **Educate employees** on CO risks, symptoms and emergency procedures, and train them on reporting suspicious odors or symptoms. They should also be trained to avoid overexertion if they suspect CO poisoning and to leave contaminated areas.
- **Ensure proper ventilation** in enclosed spaces where fuel-burning equipment runs.
- **Install CO detectors** in areas near potential CO sources (e.g., boiler rooms, garages, kitchens) and regularly test and replace their batteries. If an employee is at a heightened risk of CO exposure, provide them with a personal CO monitor.
- **Prohibit the use of gas-powered equipment indoors or in poorly ventilated areas**. When outdoors, CO-producing equipment should not be run near open doors, windows or air intakes to help prevent CO infiltration.
- **Provide personal protective equipment** to employees who work in areas with potentially high CO concentrations and train them on how to properly use it.
- **Develop and communicate an emergency plan** for CO incidents. Such a plan should include procedures for evacuation and providing medical assistance.
- **Consider alternative power supplies** (e.g., batteries or electricity) instead of gas-powered tools or equipment.

Conclusion

Being aware of the risks CO presents and taking proactive steps to eliminate or mitigate those hazards can help employers ensure safe working conditions for their employees.

For more information, contact us today.

This document is not intended to be an exhaustive source of information nor should any discussion or opinions be construed as legal advice. Readers should consult legal counsel or a licensed insurance professional for appropriate advice.

Risk Strategy Solutions

The Benefits of Cybersecurity Awareness Programs and How to Implement Them

Cybersecurity awareness programs provide informative training sessions on cyberthreats and cybersecurity best practices. These programs aim to educate individuals and organizations about the importance of maintaining a secure online environment and the risks of cyberattacks. Thus, implementing a comprehensive cybersecurity awareness program can create a strong cybersecurity culture and provide employees with essential training on recognizing and preventing costly cyberattacks.

Cybersecurity Awareness Program Benefits

In addition to reducing the likelihood of successful phishing and social engineering attacks and other cyber incidents, cybersecurity awareness programs can offer the following benefits to businesses:

- Improved employee understanding of cybersecurity risks and best practices
- Assistance in avoiding financial, legal and reputational consequences related to cyber incidents
- Faster incident response and mitigation due to employee preparedness
- Increased customer trust by demonstrating a commitment to data protection
- Potential insurance cost savings by reducing the likelihood of breaches and subsequent claims

Implementation Tips

Businesses must use several strategies when implementing cybersecurity awareness programs, including:

- Obtaining support from leadership by securing buy-in from executives
- Promoting the program by generating interest and providing communications through various channels
- Tailoring training content to the specific needs and risks of the organization and enlisting assistance from IT professionals to help identify and prioritize areas to cover
- Improving employee engagement using various training methods, including interactive modules, simulations, real-world examples and gamification
- Providing incentives or awards for participating in and completing exercises to help increase participation
- Regularly conducting, updating and reinforcing training to inform employees about the latest security threats and help ensure employees are equipped to handle evolving security risks
- Offering chances for employees to apply skills in real-world scenarios to help solidify their cybersecurity knowledge
- Measuring progress with baseline and ongoing assessments, gathering feedback, and continuously improving the program as the cybersecurity landscape evolves

Conclusion

A robust cybersecurity awareness program offers several benefits to businesses, and implementing one can improve an organization’s overall cybersecurity culture. Businesses can reduce their cyber risks and safeguard their finances, data and reputations by taking the time and initiative to ensure their program’s effectiveness.

For more information, contact us today.

Over 90% of all cyberattacks begin with phishing, according to the Cybersecurity and Infrastructure Security Agency. The agency notes that technology can be used to mitigate phishing attacks and users can be trained to better recognize phishing emails.