WORKPLACE SAFETY

NEW LAW ADDS CRIMINAL LIABILITY FOR SOME VIOLATIONS

A NEW LAW that takes effect Jan. 1, 2027, could subject California employers who interfere with Cal/OSHA inspectors or cause serious workplace injuries to criminal charges.

AB 2321 expands criminal liability for willful safety violations that cause worker injuries. It also strengthens requirements for Cal/OSHA investigations and referrals to prosecutors.

The new law will greatly raise the stakes for employers, who need to ensure they are abiding by state workplace regulations and keeping their workplaces free of safety hazards to avoid prosecution.

Expanded criminal penalties

The law makes it a misdemeanor to willfully resist, obstruct, impede or interfere with Cal/OSHA inspectors performing their duties or to willfully violate related court orders.

Violators may face up to six months in county jail, a $5,000 fine or both.

The legislation also expands criminal liability for employers and managers cited for willful safety violations after a serious injury, illness or exposure. Previously, the law applied to violations resulting in death or permanent or prolonged bodily impairment.



Possible fines for violations

Depending on the circumstances, criminal penalties may include:

- Up to one year in county jail and a $100,000 fine.
- Up to three years in state prison and a $250,000 fine.
- Fines of up to $1.5 million for corporations and limited liability companies, with higher penalties for certain repeat offenses.

More investigations and prosecutor involvement

AB 2321 also strengthens the role of Cal/OSHA's Bureau of Investigations and increases coordination with law enforcement. Key changes include:

- **Mandatory investigations:** The BOI must investigate serious injuries, illnesses or exposures involving willful citations.
- **Earlier prosecutor notification:** Cal/OSHA must immediately notify the appropriate prosecuting authority of workplace fatalities, serious incidents involving five or more employees or requests for prosecution by the BOI.
- **Emergency responder reporting:** Police and fire agencies responding to qualifying workplace incidents must immediately notify both Cal/OSHA and the county district attorney's office.

These changes could increase the likelihood that serious workplace accidents lead to criminal investigations and prosecution.

What employers can do

- Review your Injury and Illness Prevention Programs and procedures for handling Cal/OSHA inspections and serious workplace incidents before January.
- Designate someone to coordinate inspections, train supervisors to cooperate with inspectors and ensure safety records are organized and accessible.
- Promptly address known hazards, document corrective actions and establish procedures for preserving evidence following serious incidents.
- Seek legal guidance on access disputes and involve counsel early following serious workplace accidents.

Continued from page 1

Insurance Can Help Cover the Costs of a Cyber Attack

The latest developments are yet another reason that businesses secure cyber insurance policies, which may cover the costs of:

Data breaches and forensics: Pays for IT experts and forensic investigators to figure out how a breach happened, stop the attack and secure your systems.

Data recovery and restoration: Covers the cost of recovering, rebuilding, or restoring lost or corrupted data and digital assets.

Customer notifications and public relations: Reimburses you for notifying affected customers (mailing, call centers) and hiring public relations specialists to manage reputational damage.

Cyber extortion and ransomware: Can cover ransom demands (when approved) and the cost of negotiators dealing with extortionists.

Business interruption: Replaces lost income and covers ongoing fixed expenses if an attack or system failure forces you to pause operations.

Funds transfer and service fraud: Covers the cost of lost misdirected funds from funds transfer fraud scams where criminals impersonate a company executive to facilitate a fraudulent transfer.

Call us for a review of your cyberattack exposure. 800-234-6787