April 2022
Volume 7 | Issue 2

BOLDS RISK & INSURANCE SERVICES

BoldsRisk

CONSTRUCTION SECTOR

Inspections of Public Works Projects Increase

CONSTRUCTION COMPANIES and contractors that work on publicly funded projects in California can expect increased enforcement activity from a new task force that will target businesses that fail to comply with labor and workers' compensation laws.

The main focus of the Labor Enforcement Task Force is public works contractors, which the Department of Industrial Relations defines as prime contractors and subcontractors that work or bid on public works projects.

Targeting wrongdoers

The task force, which has been funded with $30 million thanks to legislation passed in 2021, includes representatives from a number of agencies under the DIR, which are pooling their resources and sharing information to ferret out employers that fail to:

- **Carry workers' compensation insurance.** All California employers are required to carry workers' comp insurance to cover their employees in case they are injured on the job.
- **Comply with Cal/OSHA standards.**
- **Comply with apprenticeship rules.** All public works contracts valued at $30,000 or more carry an obligation to hire apprentices, unless the craft or trade does not require the use of them, as indicated in the corresponding prevailing wage determination. You can check the prevailing wages for apprenticeships by county and job description here.
- **Comply with wage and hour laws and prevailing wage laws for public works projects.** Employers must pay all workers employed on qualifying public works projects the prevailing wage for their lines of work. Those prevailing wages are determined by the DIR according to the type of work performed and the location of the property.
- **Comply with skilled and trained workforce regulations for public works projects.**

Employers that fail to comply with public workers requirements can face civil penalties as well as criminal charges.The same goes for employers that don't carry workers' compensation coverage or underreport the number of workers they have in order to reduce the premium they pay.

And employers that fail to comply with Cal/OSHA safety requirements can be cited and fined for those infractions.

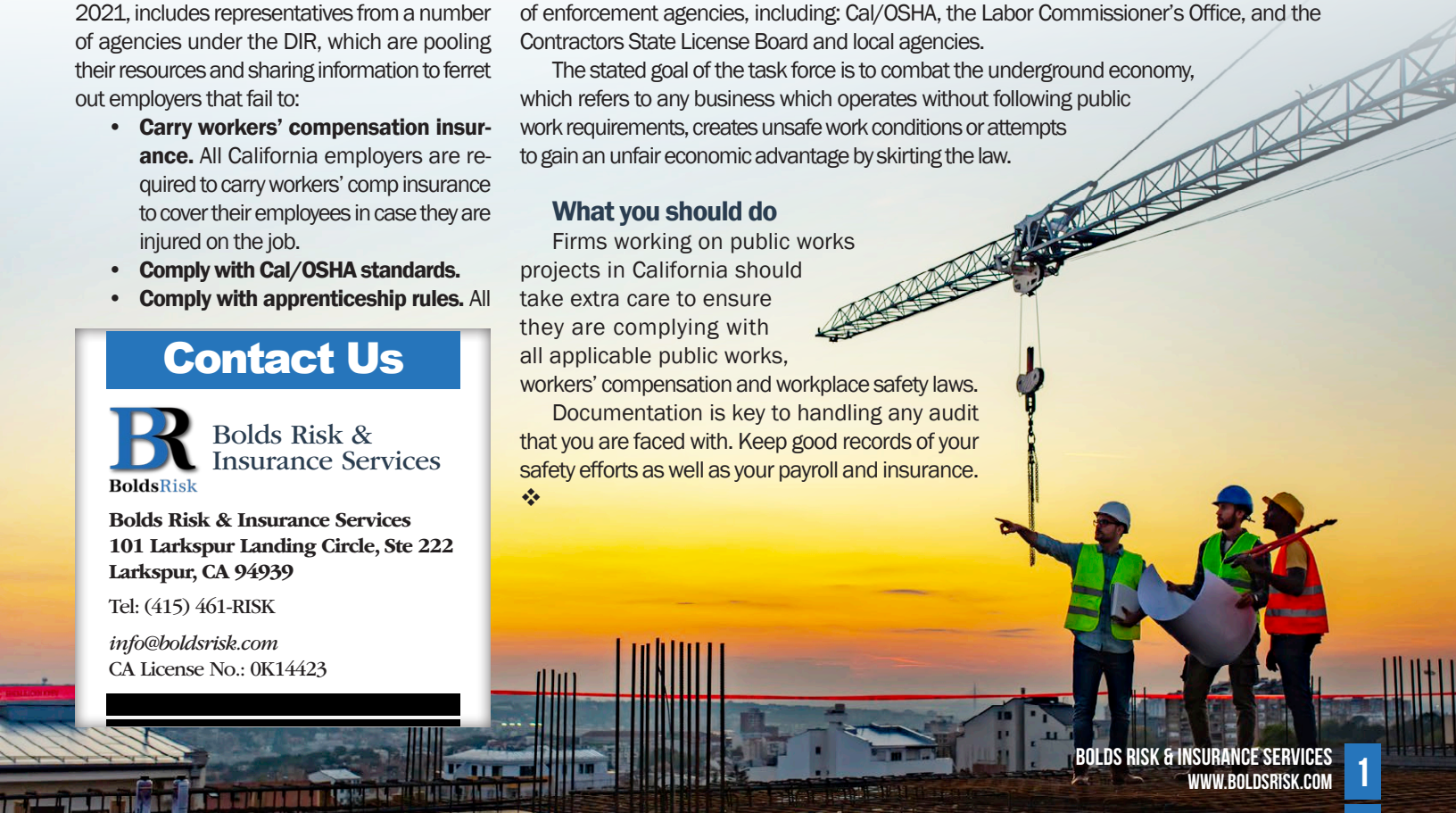
The Labor Enforcement Task Force, which operates under the direction of the DIR, is a coalition of enforcement agencies, including: Cal/OSHA, the Labor Commissioner's Office, and the Contractors State License Board and local agencies.

The stated goal of the task force is to combat the underground economy, which refers to any business which operates without following public work requirements, creates unsafe work conditions or attempts to gain an unfair economic advantage by skirting the law.

What you should do

Firms working on public works projects in California should take extra care to ensure they are complying with all applicable public works, workers' compensation and workplace safety laws.

Documentation is key to handling any audit that you are faced with. Keep good records of your safety efforts as well as your payroll and insurance. ❖



Contact Us

Bolds Risk & Insurance Services
BoldsRisk

Bolds Risk & Insurance Services
101 Larkspur Landing Circle, Ste 222
Larkspur, CA 94939

Tel: (415) 461-RISK

info@boldsrisk.com
CA License No.: 0K14423

INTERNAL SUPPLY CHAIN

Planning Ahead for Equipment Failures Can Save You

AS A BUSINESS owner you already know you need to protect against and plan for external supply chain risks. These risks are often out of your control as they can affect suppliers or transportation providers, as well as transportation networks and infrastructure.

However, you also have internal supply chain risks, which you are better able to control. These risks can affect a variety of businesses from manufacturers to retailers and restaurants – and any business that has some type of revolving stock.

It could be vital to the survival of your business that you prepare for internal risks such as machinery and equipment breakdowns.

Knowing the right steps to take ahead of time can save you from making a bad situation worse or significantly delaying the resumption of operations. All of that, of course, amounts to extra costs for your operation, including the potential for lost revenues.

If you prepare for a failure of a key piece of equipment or machinery, you also won't be scrambling trying to figure out your next step in times of internal disruption or crisis. Making decisions at such times can often lead to more problems and costs.

Your risk management plan to deal with such failures should include:

1. A list of key equipment

- Production machinery, including gear sets, motors, compressors, belts and fans.
- Boilers and pressure vessels.
- IT and communications systems, including wiring and cables.
- Electrical equipment or system, including transformers, switch boxes, cables, wiring and motors.

2. An inventory of spare parts

Optimally, you should keep all the key spare and replacement parts for your main systems on site. You can ask the manufacturers or service companies of those systems to assist you in having an emergency inventory on hand.

Still, it may not be feasible to have all items on site. In that case, you should compile a list of the other parts that could break and need replacement, and how to quickly order them from the correct supplier. You should include on this list the cost of those items and delivery times – and update the list at least every year.

3. Plan for renting replacement equipment

As part of your planning, you should obtain quotes from companies that rent out the same type of equipment or machinery that you use, and update the quotes every year. The quotes should include all pricing like transportation and set-up fees, as well as estimated time from ordering to delivery and start-up.

Don't forget to include alternative suppliers.

4. Repair firms

You should also have at the ready information on the various contractors that are able to repair equipment that's broken down. The information should be listed by equipment item and should include contractor capabilities, contact information and availability.

Again, you should update this information every year.

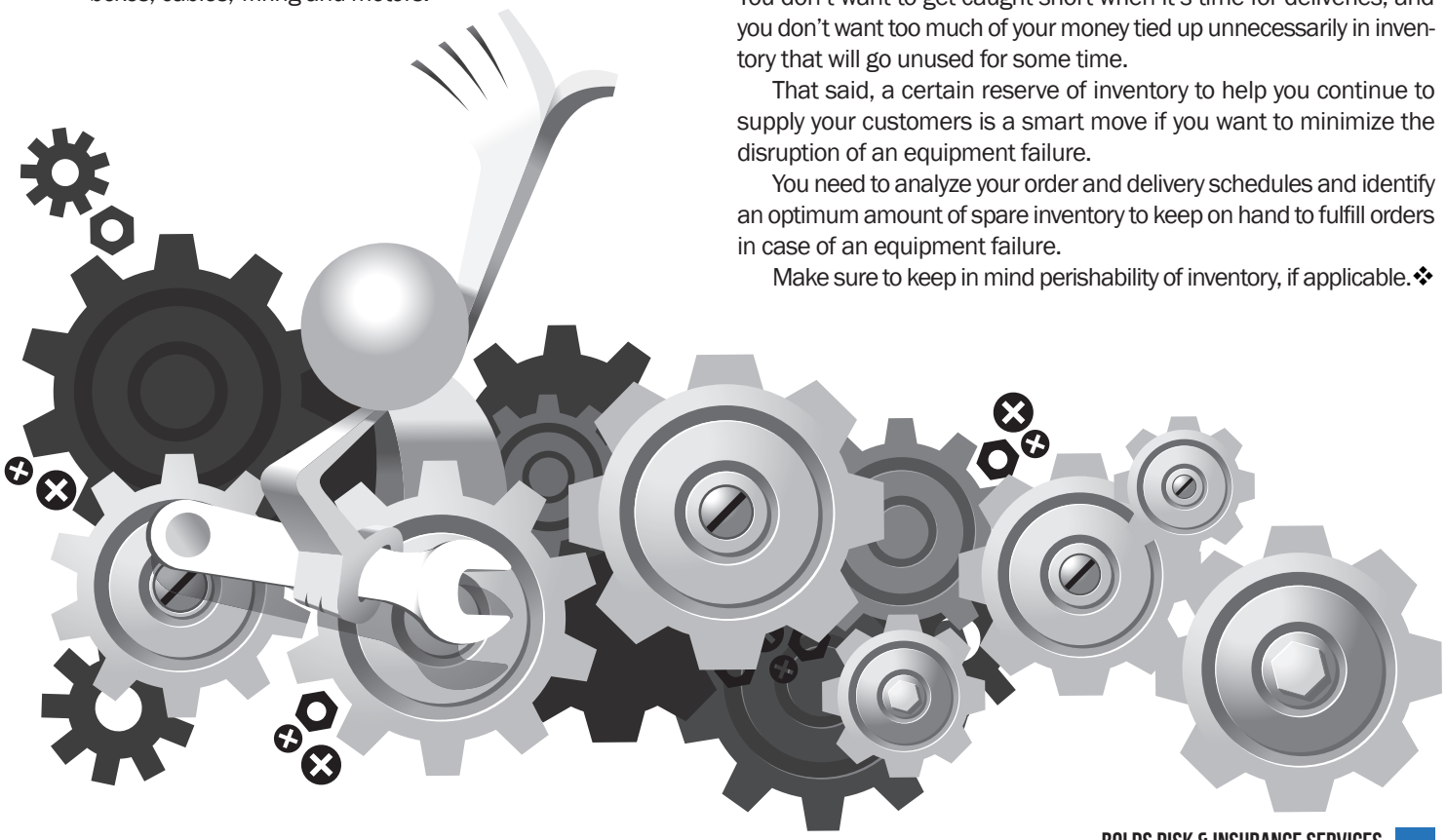
5. Inventory

The dilemma for many businesses is how much inventory to carry. You don't want to get caught short when it's time for deliveries, and you don't want too much of your money tied up unnecessarily in inventory that will go unused for some time.

That said, a certain reserve of inventory to help you continue to supply your customers is a smart move if you want to minimize the disruption of an equipment failure.

You need to analyze your order and delivery schedules and identify an optimum amount of spare inventory to keep on hand to fulfill orders in case of an equipment failure.

Make sure to keep in mind perishability of inventory, if applicable.❖



RISK MANAGEMENT

Don't Let a Subcontractor Derail Your Safety Efforts

ONE OF the biggest challenges construction businesses face is preventing subcontractors' and suppliers' poor or non-existent safety practices from denting their own safety program.

While you may consider a number of factors when vetting a new subcontractor or vendor, one area that is often overlooked is their workplace safety practices.

This mistake can cost you dearly if one of their workers causes an incident at your worksite. In addition to an injury to one of your own employees, you could get a visit from an Occupational Safety and Health Administration inspector.

The National Safety Council's Campbell Institute recently conducted a study of organizations with excellent safety records to identify the best practices for subcontractor and vendor safety.

As part of the study it identified five steps during a contractor or vendor relationship when it's incumbent on a hiring company to evaluate the workplace safety habits of their business partners.

Prequalification

The institute recommends looking at more than just a company's experience modification rate. It says safety-minded firms assess subcontractors in multiple areas, such as their total recordable incident rate, fatality rate, days away from work for injured workers, restricted or transferred rate, and other OSHA recordables for the last three years.

Many firms also ask for environmental reports, written safety programs, permits, licenses, and continuous improvement programs.

Pre-job task and risk assessment

Before a subcontractor begins work, institute members recommend having a method for evaluating the risk of the work that is to be performed. Doing this can help you understand the scope of the work and give you a chance to put into place a new written safety program if the risk is deemed high.

Most importantly, subcontractors should be required to adhere to the same safety standards as your company.

Training and orientation

You should require safety orientation and skills training for subcontractors before they step onto your jobsite.

Also, if they are doing highly specific work, you should ensure they have any required permits or special training. Some of the jobs that fit into that category are confined-space entry, electrical work, hot work, energy control, forklifts, and elevated work.

Job monitoring

Many safety-minded companies monitor work with daily checklists, pre-shift tailgate or safety meetings and weekly walk-through inspections. Some of the companies surveyed for the study also require contract employees to submit a certain amount of safety observations and utilize mobile applications to report non-compliance or unsafe conditions.

Also, you need to keep up-to-date incident logs, as this is crucial to monitoring subcontractor safety during a project.

Post-job evaluation

Conduct a post-job evaluation. During this phase look at safety, customer service and the quality of the finished work, and use those factors in determining the subcontractor's eligibility for future contracts. ❖

GROWING THREAT

Funds Transfer Fraud Hits Small Firms the Hardest

WHILE RANSOMWARE is making the headlines as the major cyber threat, small and mid-sized businesses are increasingly being targeted by lower fraud that dupes them into wiring criminals funds, according to a new report.

These funds transfer fraud crimes involve hackers gaining access to a firm's mailbox and extracting payments that go into their accounts.

Companies should have in place proper systems safeguards to combat these attacks, and that includes regularly training staff on how to identify these attempts to steal funds.

By The Numbers

69%	Average jump in losses from funds transfer fraud from 2020 to 2021
105%	Average jump in small firms' losses from funds transfer fraud from 2020 to 2021
$309,000	Average initial losses from funds transfer fraud for small firms in 2021

Source: Coalition's "2022 Cyber Claims Report"

How it works

Criminals will often try to penetrate your servers by sending "spearphishing" e-mails. These messages look like they're from a trusted sender to trick victims into revealing confidential information.

They may also send malicious e-mails in the hope that an employee clicks on a bogus link. The link then releases malicious software that infiltrates company networks and gains access to legitimate e-mail threads about billing and invoices.

Once the criminals have access to your business mailbox, they can manipulate your contacts and modify payment instructions. They may also use their access to your systems to send e-mails that appear to come from a known source making a legitimate request.

Protecting your enterprise

- Don't click on anything in an unsolicited e-mail or text message asking you to update or verify account information. Look up the company's phone number on your own (don't use the one a potential scammer is providing), and call them to ask if the request is legitimate.
- Carefully examine the e-mail address, URL and spelling used in any correspondence. Scammers use slight differences to trick your employees and gain your trust.
- Be careful what you download. Instruct your staff to never open an e-mail attachment from someone they don't know, and to be wary of e-mail attachments forwarded to them.
- Set up two-factor (or multi-factor) authentication on your accounts.
- Verify payment and purchase requests in person if possible, or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
- Be especially wary if the requestor is pressing you to act quickly.

Source: Federal Bureau of Investigation

Insurance options

The best option for coverage is a commercial crime insurance policy. Most of these policies cover acts like:

- Employee dishonesty
- Computer and funds transfer fraud
- Forgery or alteration
- Money and securities theft
- Theft of client's property.

Some policies may exclude funds transfer fraud, or they may have lower sublimits for such acts. In such cases you may need to get a policy extension to cover the risk.

There is also cyber liability insurance, which covers direct losses resulting from cyber crime. But these policies will often exclude coverage for social engineering attacks, which are the kinds that the criminals behind funds transfer fraud use.

You may be able to purchase a rider to your cyber liability policy that would cover these crimes. ❖