No accident
Identifying the five biggest safety risks to your workers

Construction innovators can still claim the research tax credit

Evaluate the risks of joint ventures carefully

THE CONTRACTOR’S CORNER
Is risk management software a worthy investment?

Check out our Construction Industry Group page and construction blog.
laporte.com/industry/construction
orgive the pun, but a culture of safety doesn’t happen by accident. Planning is key to minimizing the hazards and practices that lead to mishaps and disasters. To help categorize the most widely occurring — and lethal — risks on any construction site, let’s focus on what OSHA calls the “fatal four” and then add one more.

1. Falls
Falls are the leading cause of death in construction. Contributing factors typically include unstable working surfaces, misuse of — or failure to use — fall protection equipment, and human error. During preconstruction of a given project, think about what the job will entail. What kind of equipment will be used? What will the conditions be (for example, wet or icy)? Will employees work from heights of six feet or more above ground level? Will they use ladders or stairways?

With these questions answered, you can determine what measures to take. For instance, you may need to deploy aerial lifts or elevated platforms to provide safer elevated working surfaces. You should inspect ladders before use or ensure stairways have treads and handrails. Using perimeter protection (such as safety nets or guardrails with toeboards), fall arrest systems (body harnesses), clearly marked floor opening covers and restraint systems can prevent many deaths and injuries from falls.

2. “Struck-bys”
Construction workers can be struck by many things: heavy equipment and vehicles; falling, swinging or flying objects; or bricks or cinder blocks tumbling from unfinished walls. Even dropping a small tool could cause serious — even fatal — injury. Ensure your workers are wearing high-visibility clothing, hard hats, and appropriate eye and face protection. Tool tethering is also a best practice to follow.

Vehicles and equipment are particularly dangerous hazards to address. For instance, “backover” incidents occur when a backing vehicle strikes a person. Train workers on the ground to act as spotters, or use warning devices such as in-vehicle display monitors and radar or sonar proximity detection devices. Other strategies include strictly separating employees on foot from operating equipment (where possible) and creating internal traffic control patterns to prevent vehicles from needing to back up.

3. Electrical hazards
Workers face many electrocution risks on job-sites, including exposed or faulty wiring, hidden power lines, and wet conditions while outlets are exposed. Yet electrical hazards are arguably among the most overlooked risks — probably because we all plug and unplug items into and from outlets every day without thinking about the dangers.

Virtually every contractor knows to contact local utilities to identify buried lines before digging. But take extra care with such routine steps when working on a “rush job.” Ensure workers are duly informed of these locations as well as taught to maintain safe-distance requirements from power lines — especially when operating equipment and working on ladders, scaffolds and other platforms.
If you don’t have one already, be sure to set up a system for regularly checking electrical tools and equipment for OSHA compliance, as well as damage and defects. For example, extension cords must have grounding prongs. Electrical tools must be properly grounded, too, unless they’re double-insulated. Promptly replace frayed, damaged or worn cords and cables.

4. “Caught in or between”
Examples of these types of accidents include getting pinned or compressed by equipment, objects or materials. Workers can also be caught in collapsing structures or jobsite locations. And they’re often trapped in or between moving or rotating equipment, such as miter saws, conveyors and rotating pump shafts.

Being caught in or between hazards is especially common in trench and excavation sites. A general safety rule of thumb is that workers should never enter a trench or excavation that’s five feet or deeper without an adequate protective system in place (such as sloping, shoring, benching or a trench shield).

As is the case with many safety precautions, it’s not enough to mandate that they be followed. Regularly audit your own jobsites and thoroughly investigate any incidents that occur.

5. Fire hazards
A fire can be devastating, not only because it can cause injury and loss of life, but also because it can damage property and cause extensive project delays. Many construction companies now implement formal fire prevention programs to ensure all bases are covered.

Such a program would include identifying and marking hazardous materials and jobsite locations, putting up signage to indicate where fire extinguishing equipment is located, and enforcing strict policies for the storage and transport of flammable materials and substances.
Construction innovators can still claim the research tax credit

There are innovators in every industry, including construction. If your company happens to be one, you may be able to claim the research tax credit, which remains available under the Tax Cuts and Jobs Act.

Explore eligibility
To be eligible, an innovation-seeking business activity generally must do several things. First, it must relate to development or improvement of a “business component,” such as a product, process, technique or software program. It also needs to strive to eliminate uncertainty over how (and whether) the business component can be developed or improved.

In addition, the company must exercise a “process of experimentation,” using techniques such as modeling, simulation or systematic trial and error that relies on “hard science,” such as engineering, computer science, physics, chemistry or biology.

What might a contractor do to qualify for the credit? There are many possibilities. Safety is obviously a major concern in the industry. By developing safer and more efficient construction techniques and methods, you may become eligible.

Inventing a process to design buildings, features or systems that improve energy efficiency or facilitate LEED certification may also qualify. And if you happen to work in the HVAC, electrical, plumbing or lighting areas, original ideas your company uses to design or improve these systems may allow you to claim the credit.

Lastly, if your construction business is on the cutting edge of technology and involves itself in software design, it’s highly advisable to explore research credit eligibility.

Peruse your contracts
To claim the credit, you must bear at least some of the financial risk associated with the research and enjoy substantial rights to the results. Otherwise, the effort will be considered “funded research,” which is ineligible for the credit.

If you do research for a customer under a fixed-price contract, it may be more likely to be eligible for the research credit because you bear the financial risk of the work (provided you also retain contractual rights to the results). Try not to do research for a customer under a cost-plus or time and materials contract, because it may be considered funded research (which is ineligible because the financial risk remains with the customer).

Crunch the numbers
If your company does qualify for the research credit, it could receive a dollar-for-dollar, non-refundable credit of up to 6.5% of qualified cost of running your construction company. Workers’ compensation costs, for instance, can spiral out of control after just a few on-site mishaps. (For more on this, see “How to make workers’ comp costs less costly” on page 3.)

Take control
Safety is important, first and foremost, because the well-being of your workers is important. But whether your jobsites are safe also directly impacts the cost of running your construction company. Workers’ compensation costs, for instance, can spiral out of control after just a few on-site mishaps. (For more on this, see “How to make workers’ comp costs less costly” on page 3.)
sometimes a construction project is just too big or complex for one general contractor to handle alone. Joint ventures (JVs) enable two construction companies to temporarily partner up to distribute risk, apportion resources and, one hopes, share profits.

There are other reasons to consider a JV. You might need to secure additional bonding capacity or meet affirmative action compliance for a government contract. A JV may also be a good way to enter a new geographic area or market segment. Of course, there are some risks to consider.

Ideal partners
Arguably, the biggest risk of a JV occurs in the beginning of the process. If you choose the wrong partner, the arrangement may be doomed to fail.

Evaluate the risks of joint ventures carefully
to failure no matter how sound the legal and financial details.

The best JV partners complement each other’s skills and resources, as well as possessing similar goals, values and company cultures. They also must establish clear channels of communication. Only when these elements match should you move forward toward formally setting forth a legally binding agreement.

**Structure and details**

JVs typically are set up as partnerships, limited liability companies or corporations. Each entity type has different tax implications, levels of liability protection and financial reporting requirements.

An agreement should outline insurance, identify bonding and tax strategies, and provide for dispute resolution procedures such as mediation or arbitration. It should lay out day-to-day procedures and clearly describe assignments for each partner — including who’s responsible for:

- Managing daily operations,
- Ensuring safety protocols,
- Obtaining permits and licenses,
- Procuring supplies and materials, and
- Handling accounting, billing and cash transactions.

If the JV is set up for one project, then it obviously terminates on completion. But a detailed termination process should be agreed on and included in the agreement. The outline for the closeout phase needs to fully define the warranty period and when final partner distributions will occur.

**Financial aspects**

When it comes to finances, you may be able to establish rates to charge the JV for the cost of items such as labor, equipment, overhead and insurance. If you can do so, include the rates in the agreement. Rates may be based on actual costs or negotiated fixed rates for each item.

Very importantly, a joint venture agreement should outline the way cash distributions from JV profits are made to partners. It’s prudent not to permit cash distributions until the project is more than halfway complete to ensure you have the cash flow for job costs.

Unforeseen conditions can create extra costs, so there should be a provision requiring partners to fund the JV in the absence of sufficient revenues. If one partner can’t contribute to the funding, the other partner(s) may be required to step in and cover that portion. Thus, the financial stability of potential partners should be disclosed before an agreement is signed.

**Who can help?**

A well-planned JV can be a big step forward for some construction companies. A poorly planned or structured one, however, will likely wind up as a major stumble. Consult with trusted legal and financial advisors with expertise in JV agreements before signing on the dotted line.
My construction company recently underwent an audit by the Occupational Safety and Health Administration (OSHA). Among the most important findings is that our safety and insurance documentation is inadequately organized. While researching the matter, I learned that there’s software available to help businesses with this problem. But is it a worthy investment, or would I be better off reworking my existing approach?

It’s true. Software commonly known as risk management information systems (RMIS) offers companies the ability to gather, organize, store, access and share data related to the areas you’re struggling with. Whether it’s a worthy investment is a good question that depends on your comfort with technology as well as your budget.

How it works
An RMIS stores risk and insurance data in one place — from insurance policies and statements to safety program documents and incident reports to OSHA guidance and audit results. The system links employees, subcontractors, developers and vendors to site locations so you (or anyone handling risk management) can filter and track the data in various ways: by date, project, location, vendor, and insurance policy or coverage type.

You can use this information to allocate costs across projects or locations. Plus, the system enables you to generate risk-management and safety-related reports. Some systems also can connect with third-party systems to digitally share information.

How it helps
Here are some examples of how an RMIS might help a contractor:

Easier subcontractor insurance approvals. General contractors can create risk profiles outlining subcontractors’ insurance requirements. Then, the subcontractors themselves may use the RMIS Web portal to enter their insurance information and upload documents. The system can then notify a subcontractor via email or text whether the submission was accepted.

Instant incident reports. Project managers and other workers with system access can report safety incidents from anywhere with GPS coordinates. They can take pictures and videos with their mobile devices and attach those as well. The system maintains a log of such reports for easy access, report generation and sharing.

More thorough inspections and investigations. Many RMIS include an audit tool that automates documenting site inspections and accident investigations. Safety personnel use electronic forms to enter information, which are uploaded directly from the jobsite. When inspections, audits or investigations are completed, the system can even automatically generate corrective actions and assign them to various individuals.

Due diligence
To determine whether you should spend the money, you’ll need to perform thorough due diligence. Specifically, assess whether you and your staff can get the proper training to learn the system and ensure that you’re motivated to use it long term. Naturally, your budget must have room for the purchase as well.
Hackers: What You Need to Know

Cybercriminals are after one thing: **money**.

To take money out of your organization, all a good hacker needs is an opening – just a sliver of an opening – to your data. As a player in the construction industry, you have more than enough data (and access to cash) to be an appealing target.

**What Hackers Want and How They Get It**

To hackers, sensitive and personal data is the same as cash. Your workers’ tax, payroll, and personal information can be sold; your clients’ credit card data can be auctioned to the highest bidder; and the sensitive matters you discuss with your business partners can be used as fodder for blackmail.

Cybercriminals have advanced tricks up their sleeve to get this information.

**Wire Fraud**

Money that’s in transit will be tempting. Frequent wire transfers, ACH payments, and online banking dealings will attract hackers.

**Social Engineering**

If simply stealing money isn’t an option, cybercriminals can manipulate your workers into transferring them money or giving them access to your systems. Phishing, pretexting, and baiting are social engineering schemes that cybercriminals will use to coerce your employees.

**Good, Old Fashioned Hacking**

Sometimes, cybercriminals choose to simply barge their way into your systems. If they can breach your security defenses, they can install Trojan software to take control of your computers, worms that will self-replicate to take over your network, or spyware to monitor future keystrokes.

**Solutions**

First things first: perform a risk assessment. If you are aware of your vulnerabilities, you will know how to shore up your defenses.

Once you know your risks, look for the simplest solutions. Often, hackers will move on from your systems if they see that you are actively protecting them; they know that they can find easier targets elsewhere. Some simple fixes are:

- Update systems and patch software regularly
- Employ two-factor authentication
- Require password complexity
- Restrict access to your key systems to only certain workers
- Review administrative privileges regularly
- Provide your employees with cyberattack awareness training
- Purchase cyber insurance
- Get buy-in from all leaders of your organization

Global cybercrime is at an all-time high. According to a study by the Center for Strategic and International Studies, it is estimated to cost businesses up to $600 billion each year. For help in developing an action plan to mitigate your risk, please contact a member of the LaPorte Risk Advisory Services team today.