Risk Control

UNFORESEEN PERILS OF THE PANDEMIC: CURRENT INSURANCE CONDITIONS, CHANGING CONSTRUCTION TRENDS AND REMOTE WORKERS

The COVID-19 pandemic continues to impede construction operations. Supply chain disruption, skilled labor shortages and project cancellations make scheduling, timely project completions and profitability difficult to obtain. At the same time, construction firms report a change in the balance of residential vs. nonresidential construction projects. All produce new exposures for firms building and managing construction projects.

Residential Construction Exclusions.

The National Underwriter magazine (October 2020), in *Rising Uncertainty*, suggests a better job recovery for residential over nonresidential construction. From August to September 2020, nonresidential construction had a net gain of 4,000 jobs, while residential construction experienced a gain of 22,000 jobs, the largest for specialty trade contractors. This pattern is similar to predictions made by the AIA Consensus Construction Forecast Panel, which indicated that nonresidential project spending will decrease 8-percent this year and nearly 5-percent in 2021. Bottom line: residential construction will be an important driver of construction jobs and projects.

However, the insurance carriers – driven mainly by construction defect claims – have the option to place residential exclusions on commercial general liability policies. Used mostly by nonadmitted (Excess or Surplus lines) insurers, these exclusions eliminate coverage for operations arising from work done on residential property. As expected, exclusions differ depending on the underwriter's concern about the risk, for example, they can remove coverage for:

- Any type of residential construction.
- Single family homes, coops and condos.
- Multifamily structures.

Residential exclusions can also be found in endorsements eliminating coverage for a designated operation, ("Excluded Operations" endorsement), or by listing only the specific operations the policy will cover ("Designated Operations") and not including residential work. Some of these exclusions include an exception for repairs or remodeling but still exclude new construction work. These exclusions not only limit coverage for the policyholder, but also for entities who expect additional insured status as upstream parties (owners and general contractors) from subcontractors and others.

Hardening Insurance Market – Expect More Onerous Contract Terms

Premium increases (especially in the umbrella/excess and commercial auto markets), unfavorable coverage terms and unwanted exclusions will blunt profitability for many firms, depending on operations, loss experience and the carrier's appetite for the risk. Expect upstream parties to look for additional ways to transfer risk, whether through liability limitations in contract terms, or insurance requirements with demands for higher limits and additional coverages not normally required, such as

Owners Contractors Protection (OCP) policies or a blanket request for property coverage and an expanded list of prohibited policy exclusions. Make certain that insurance requirements, especially on revised contracts or contracts with new customers, do not contain unwanted (or unavailable) coverage limits, terms, coverages and conditions. Get your attorney involved as well.

Changes to the Employment Practices Liability (EPL) Exposure

With COVID-19 cases trending upwards this fall, employers are operating in an environment fraught with issues that can lead to employment liability claims. Questions concerning disability and COVID-19 related medical inquires; confidentiality issues; hiring, rehiring and onboarding, and requests for accommodations from affected workers need to be evaluated and answered.

If unchecked, harassment directed against individuals who had the disease, or are in a high-risk group (such as older workers) will lead to complaints to the Equal Employment Opportunity Commission (EEOC) and/or state human rights offices. Although many businesses have reopened, unemployment may surge again if restrictions are imposed this winter due to a resurgence of the disease. This is especially true for hospitality and brick and mortar retail stores. Layoffs, furloughs or mandatory reductions in hours increase the likelihood of wrongful termination claims against employers.

Remote Worksites – Workers' Comp and Cyber Liability

Workers' Compensation covers employees who are injured or become ill as a direct result of their job. In most cases, compensability (when the accident and resulting injury or illness is covered by the law) is straightforward. However, for employees working remotely the issue is not as clear. Employers do not have the same control over the employee when they are working away from the office. To mitigate accidents, employers can adopt and enforce a remote work policy. Policies differ depending on the type of work being done, but most policies address:

- A designated, safe workspace.
- The employee's scope of work.
- Work hours.
- Required conditions and prohibited activities (such as the need for child care).
- Benefit and compensation changes, if any.
- Reimbursement for supplies.
- Communication with managers and supervisors.
- Accident reporting.

Mitigation and prevention also apply to cyber threats. With employees working remotely, cyber criminals have stepped-up their efforts to breach security and gain access to personal information, passwords and to hack into financial systems.

In April, the FBI reported a 400-percent increase in the number of complaints to the Internet Crime Complaint Center (IC3) since the inception of the COVID-19 pandemic in early 2020. While all the reports were not COVID-19 related, many were. If states and local governments reinstate mandatory shutdown and restrictions, expect cybercrime to increase as the number of remote workers rebound to their pre-summer levels. Now is the time to open a discussion with your IT vendor or company IT manager.

On November 1, 2020, Construction Executive (https://constructionexec.com/) in *CE this Week*, gave four suggestions geared for companies to reduce incidents of cyber-attacks:

1. Train staff in basic cyber security. Employees should recognize phishing attacks, spoofing, and whether their computer or laptop has been hacked.
2. Beef up IT security and IT staff. Many companies are now installing multi-factor authorizations for system access.
3. Update company policies concerning computer use.
4. Purchase cyber insurance. Cyber coverage insures against financial loss from third-party claims, the cost of notification expenses and damage to networks and data.

Other suggestions include: having employees install software updates and patches, prohibiting storage of company data on personal devices (using a document storage service), requiring strong passwords for home Wi-Fi networks, and quickly reporting any cyber-attacks or attempts to the company's IT manager. When possible, provide employees with company-owned IT equipment and prohibit the use of personal equipment for company business. IT specialists often follow industry accepted standards when initiating a loss prevention model, for example, the NIST model.

The Cybersecurity and Infrastructure Agency of the U.S. government published information about recognizing threats from email and communications, malware, phishing attacks along with prevention strategies at their website: https://us-cert.cisa.gov/ncas/tips.