FOA & SON
·1861·
INTERNATIONAL INSURANCE BROKERS

CORPORATE HEADQUARTERS • NEW YORK, NY • TEL 212 432 1234
EASTERN REGIONAL OFFICE • MELVILLE, NY • TEL 516 228 1234
PERSONAL LINES CENTER • VALHALLA, NY • TEL 914 773 4321

THE INSURANCE NEWSLETTER

Fall 2015

Contractors Technology Risk

Here's the scenario: A large (100+ employees), long established and well respected mechanical contractor has an agreement with a major national retail chain for maintaining cooling and refrigeration equipment in a number of the chain's stores in their territory. As part of their service contract the contractor installed automatic sensing equipment on the each unit and set up the monitors to remotely report status back to the contractor, over the internet, of all monitored equipment. In the event of a failure or breakdown the contractor would then be able to respond immediately and dispatch service personnel to deal with the problem. To effect this automatic communication the contractor obtained permission from the chain to access the chain's IT system and internet connection, and set up their equipment monitors to report back to the contractor through that connection.

Hackers break into the contractor's computer system. It's later determined that the only security software used by the contractor was a free version downloaded from the internet. Using the access granted to the contractor by the retailer, the hackers then penetrated the retailer's IT system. Having gained access through this unprotected back door, the bad guys remotely installed a bit of malicious code at each point of sale terminal in the retailer's stores, both those within the contractor's territory and elsewhere. This particular bit of code recorded credit and debit card numbers as they were swiped, stored them temporarily, then periodically transmitted them, through the contractor's access point and system, to the black hats. Over a couple of weeks hundreds of millions of records were thus stolen, at huge cost to the chain.

The story is true. The retail chain was Target, and by now almost everyone has heard of this massive breach in early 2014. Details of the hack and how it was done are widely available with a simple Google search.

This was obviously a ruinous breach of security that has resulted in hundreds of millions of dollars of loss to Target. Liability for the loss was easily traced back to the contractor. The contractor reportedly had a standard commercial general liability insurance policy that insured for property damage liability. Here's the problem with that, though: the property damage coverage in the standard CGL policy covers damage to tangible property. Computer records and credit card numbers are not tangible property, so any liability falling to the contractor for this loss, as described, would not be covered by a standard CGL policy. In fact, there has been no report in the insurance press of any insurance company paying any property damage claims related to this incident.

This is an extreme example, not so much because of the circumstances of the loss, but because of it's size and the publicity it got. Examples abound of similar occurrences and claims, not covered by standard CGL policies, that contractors are incurring all the time. They can be ruinous; the contractor in this case was visited by the FBI and Secret Service, among others, and would have had no insurance coverage for any of the massive amounts of litigation spawned by the breach. Smaller claims can be equally damaging, but with the rise of technology and the digital information age, many contractors are not aware of the limitations in their CGL policies and the risks they face from the possibility of claims of loss or damage to the types on nontangible property involved here.

Contractors (and others) can find insurance to cover losses like these; coverage is available. Unfortunately, there are a couple of practical problems with this new type of insurance. First, most contractors resist the idea of buying another insurance policy; second, project owners and construction managers have not yet caught up to the fact that this exposure exists and that the contractors they deal with have no insurance for these increasingly frequent types of claims. For the most part they have not yet begun

to require it, and for those few who might try, go back and read the first point; contractors push back because "no one else asks for this".

Stay tuned. This is an issue that will be evolving over the next few years.

Trends in General Liability Insurance

The Insurance Services Office (ISO) is the industry organization that drafts standard insurance policy forms used by most insurance carriers. Because laws, exposures and claim trends continually evolve, standard policy form updates and revisions are introduced regularly, generally on a three year cycle. GL policies were last revised by ISO in 2013, so 2016 would be the next year we could expect to see some changes. Insurance companies will often tip off the types of changes that might be expected at the next revision by the types of exclusions or amendments they add to policies; based on what we see in many current GL policies these are some trends we might expect to see incorporated into the next general liability policy revisions.

Technology Exclusions

The world has become digital, but insurance is still analog. GL policies have always been written and interpreted to cover only tangible injuries or damage. In the context of property damage liability especially, that puts GL policies at odds with a world where much valuable property now consists of bits and bytes, that is, intangible (but still valuable) information or data.

The case discussed in the preceding article is a perfect example of the problems this creates. The current 2013 edition of the CGL form already specifies property damage only covers tangible property, but due to the growth of incidents like the one described earlier underwriters are now routinely adding an electronic data exclusion, further underlining their intent to cover only damage to tangible property.

Expect the next policy revision to incorporate wording that further clarifies the policy intent to cover only liability for damage to tangible property.

Total Pollution Exclusions

The current form excludes claims arising from pollution, but there are a number of significant carve backs. Examples: pollution arising from a hostile fire (the smoke and water runoff from a structure fire is certainly a pollutant) is covered. Pollution in building heating or cooling systems (119 affected individuals and 12 deaths from the Legionnaires Disease outbreak in New York City this summer) is covered. And for both the GL and Auto forms there is an exception to the pollution exclusion for fuel, lubricants and other such fluids in motor vehicles and mobile equipment. Imagine a vehicle overturning and rupturing a full tank of diesel fuel which runs off into a river; that's covered, although not pollution from any cargo the equipment is carrying.

So despite the pollution exclusion built into the form there is some meaningful coverage given back. Underwriters have been chipping away at that for a while, though; CGL policies now routinely come with asbestos, silica, and mold & fungus exclusions added, even though these things are arguably already covered by the wording of the existing pollution exclusion. Worse, in addition to these now you'll often find a total pollution exclusion endorsement added to GL policies; that takes away the little pollution coverage still given in the standard policy wording.

We'll be looking at the 2016 revision to see what changes it might bring with these exclusions.

Broad Form Indemnity Exclusions

We wrote about anti indemnity exclusions just in the last issue. Many states already will not allow, by statute, one party to indemnify another for the sole or partial negligence of the party indemnified.

For those states or jurisdictions where no such laws exist, underwriters are often attaching a broad form indemnity exclusion. All this means is that if you sign a contract where you agree to indemnify another for damages they suffer due to your negligence, you're OK; if you agree to indemnify them for their partial or sole negligence, even if in connection with work you might me doing for them, you're out of luck, your insurance policy won't respond.

Don't wait until this is built into a future CGL revision. Starting now, you should be looking at the indemnity provisions of any contract you sign. If you are assuming liability in the contract but your GL policy won't cover it, you become the insurance company, not a place you want to be.

Drones

These are popping up everywhere. There is an aircraft exclusion in the current CGL form, which has been there through many prior editions in virtually the same form.

Problem: "aircraft" is not a defined term. Is a drone an "aircraft"? Is bodily injury or property damage caused by a drone covered? Unclear.

Expect to see something addressing this in the next revision.

The thing to take away from this discussion is not that you'll be totally exposed if any of these current or future exclusions apply to you. Underwriters exclude things from policies for many reasons, but the most important reasons you'll see an exclusion is either 1) it's just not something possible to insure (think war, or nuclear explosion), or, 2) coverage is available elsewhere in a policy or form more appropriate to cover it.

By way of example of this last point, auto liability and liability for employee injuries have always been excluded from modern CGL policies. They are certainly insurable; if you need this coverage you can buy an auto or workers compensation policy. The same principal applies to technology risk, pollution and, in evolving form, drones. If you need it, you can buy it, from underwriters who specialize in those areas. Indemnity exclusions are a little more work, you just need to be sure you don't agree to assume liability for the negligence of others, but that can certainly be done.

Bottom line, these evolving and possibly imminent changes to standard policy forms are in areas where solutions are available if you need them. We are keeping an eye on them. If you think any of them might apply to you in the meantime, let's talk about solutions.

New Overtime Regulations

Last June 30th the Department of Labor (DOL) released proposed rules updating federal overtime pay regulations under the Fair Labor Standards Act (FLSA). The FLSA was first enacted in 1938 and established the first-ever national minimum wage (then, 25 cents per hour), a standard 44 hour work week (since reduced to 40), and time and a half overtime pay for hours worked past the standard work week.

These rules stood for many years, without seeing any significant updates for decades. In particular, the rules dealing with exempt employees, those defined as highly compensated employees not eligible for overtime, had not kept up with the times. Under the old rules the definition of "highly compensated" was set at a threshold of an annual income of $23,660. That old and outdated low salary threshold will increase by more than double, to $50,440 under the new rules, and will be indexed to reflect future salary growth.

The other component of exempt determination is a duties test; that has not been addressed with these changes, although it's under review. Exemptions are determined based on job duties performed and compensation received in each specific position; job titles alone don't determine the exempt or nonexempt status of any employee. The job categories eligible for exemption are currently the same; the executive, creative professional, computer employee and outside sales exemptions are still fairly straightforward, although the administrative exemption remains one of the classification categories most open to interpretation and misclassification.

So what does that mean? With definitions in the duties test not yet changed, your focus should be on looking at compensation levels, which are intended to remove many employees currently classified as exempt from eligibility for that designation. DOL estimates that 62% of fulltime salaried workers were eligible for overtime pay in 1975 under the rules then in force, but today only 8% of those same kinds of workers are eligible because of the old, low salary threshold that had not kept up with inflation and wage growth. With these changes they estimate overtime protection will extend to some 5 million additional employees. You're going to want to determine if any of them are yours.

As a final note, remember we've mentioned in the past that wage and hour employment liability claims, most often filed as class actions, are at or near the top of the list of all types of employment practices liability claims filed each year, and are forecast to reach record levels in 2015. Insurance companies writing EPL insurance want no part of them and such policies almost always exclude them; where some coverage is available, it covers defense costs only, with sublimits generally in the $100,000 to $500,000 range, max. In most cases you cannot turn to an insurance policy to cover the potential high cost (even when you win the case) of a wage and hour lawsuit.

Prevention is the key. These new rules should be the trigger for another look at your job classifications and controls.

Cyber Fraud Claims Denied

There have been several cases reported in the trade and general press about cyber fraud claims that insurance companies were able to successfully deny paying.

The stories in all were fundamentally the same: a cyber

fraudster would contact a person responsible for handling funds in an organization and induce them through fraud and deceit to transfer (often large) sums of money to a fraudulent destination. With instructions for the transfer coming from an authorized person, the banks washed their hands and disclaimed responsibility; insurance claims were filed under commercial crime policies.

We have always recommended that our clients buy a couple of inexpensive endorsements to their employee dishonesty policies, one for Computer Fraud, and the other for Funds Transfer Fraud. Details of the cases were not reported, but the insurance companies apparently argued that although the authorized user was indeed duped, since they were in fact authorized to make such transfers, there was no fraud involved in the actual transfer.

The missing step in all the cases reported was that the authorized individual who made the transfers did not take the step of actually picking up the phone and talking to the higher up who was purportedly requesting the transfer; a thirty second conversation would have nipped the problem in the bud, but instead everything was done by email. Computer Fraud and Funds Transfer Fraud coverage remains an important part of your crime policy, and it's too early to draw any conclusions from these few cases, but one lesson is clear: any organization needs to review it's internal controls governing how money is sent or received, and make sure its sound.

FOA & SON
·1861·
INTERNATIONAL INSURANCE BROKERS
68 South Service Road
Melville, NY 11747-2357

PRESORTED STANDARD
US POSTAGE
PAID
PERMIT NO 231
WINSTON SALEM, NC

The information, suggestions and techniques contained in this newsletter are believed to be accurate but are offered as information only. This firm makes no warranty of any kind, whether expressed or implied, as to the accuracy of the information or its fitness for a particular purpose.