Is There a Cyber Gap in Your Coverage for Bodily Injury and Property Damage Claims?

By John L. Watkins

What if a cyber attack caused:

- Machinery in a manufacturing plant to spiral out of control, causing a fire resulting in injuries to workers and damage to the plant;
- Refrigeration equipment in a cold storage warehouse to fail, causing food to spoil; or
- An implanted insulin pump or pacemaker to fail?

Would the manufacturer's liability insurance cover any resulting claims? The answer is a definite "maybe."

If these scenarios sound far-fetched, welcome to the Internet of Things. And this is the Internet of Things present, not future. *Everything* is networked, which in turn makes everything vulnerable to cyber attacks. Cyber attacks have been documented on factories and utilities. Last year, "white hat" hackers demonstrated they could remotely gain control of a modern automobile.

Although cyber liabilities are commonly understood to involve the exposure or compromise of medical or financial information causing economic or reputational injury, the Internet of Things means that cyber risks also involve potential claims for bodily injury and property damage. Commercial general liability (CGL) coverage is the backbone of most business liability insurance programs. CGL "Coverage A" insures against third-party claims for bodily injury and property damage.

Although insureds facing cyber claims for bodily injury and property damage would look to their CGL carriers for coverage, it is not clear how the insurers would respond. In addition to other arguments they might make, insurers have been adding endorsements to CGL policies excluding coverage for cyber-related liabilities. In 2013, the Insurance Services Office (ISO), an organization that develops form policy language, issued two endorsements for CGL policies. ISO Endorsement CG 21 07 05 14 adds an exclusion to CGL Coverage A. The exclusion states that the insurance does not apply to damages arising out of: "The loss of, *loss of use of*, damage to, corruption of, *inability to access, or inability to manipulate* electronic data." "Electronic data" includes "information, facts or *programs* stored as or on, created or used on, or transmitted to or from computer software, including systems and applications *software* … which are used with electronically controlled equipment." (emphasis added). ISO Endorsement CG 21 06 05 14 contains

identical language, but contains a limited exception for bodily injury.

In part because the definition of "electronic data" includes "programs" and "software" used with electronically controlled equipment, it is plausible, and perhaps likely, that carriers will argue that CGL policies with such endorsements do not cover bodily injury or property damage claims resulting from hacks to computers, programmable logic controllers (PLCs) or other electronic controls. Carriers might also argue that bodily injury and property damage claims tied to "bugs" in software are excluded.

If a company has taken the prudent step of purchasing cyber insurance, it unfortunately may not respond. Most cyber policies exclude claims for bodily injury or property damage, probably based on the assumption that such claims will be covered by the insured's CGL policy.

It is too early to tell if the potential cyber bodily injury/property damage coverage gap will be a big problem. Not all CGL policies use the problematic endorsements. However, one insurance executive was recently quoted as stating that a number of insurers are adopting the endorsements. It is also questionable how the courts will react. There are no reported cases interpreting the exclusionary language in the endorsements. Exclusions are generally interpreted narrowly. Courts may limit application of the endorsements, but insureds should not rely on such an assumption.

Prudent policyholders should instead take immediate action to avoid the potential coverage gap, including:

- Reviewing their CGL policies (and, if applicable, cyber policies) with experienced insurance professionals to determine whether there is a gap.
- If there is a gap, immediately exploring alternatives with an experienced broker familiar with cyber risks and insurance. Insurers are beginning to understand the issue and some are offering alternatives to cover the gap. At a minimum, brokers should be able to find coverage without the harshest CGL exclusions.

John Watkins is a partner in Thompson Hine LLP's Atlanta office. Watkins practices in the firm's business litigation and corporate practice groups, including a focus on insurance coverage. He is also an Adjunct Professor at the University of Georgia School of Law teaching Insurance Law.