The Legal Intelligencer

When Cyber Attacks Result in Physical Damage: Important Insurance Considerations

As the world becomes more interconnected, cyber attacks unfortunately are becoming more frequent, more sophisticated and more dangerous. So-called “cyber-physical attacks,” for instance, pose a unique threat—specifically, the risk of bodily injury (including, but not limited, to death) to third parties.

By **Michael H. Sampson** | August 21, 2020

Michael Sampson of Leech Tishman.

As the world becomes more interconnected, cyber attacks unfortunately are becoming more frequent, more sophisticated and more dangerous. So-called “cyber-physical attacks,” for instance, pose a unique threat—specifically, the risk of bodily injury (including, but not limited, to death) to third parties. While these attacks and this risk are not new, the insurance industry as a whole has seemingly been slow to respond to them.

"Traditional" cyber insurance policies often exclude coverage for "bodily injury," whereas marine and hull cargo insurance policies often exclude coverage, for example, for "loss, damage, liability, or expense directly or indirectly caused by or contributed to by or arising from the use or operations, as a means for inflicting harm, of any computer." And, while policyholders may have good arguments that commercial general liability (CGL) insurance policies should cover third-party liability claims arising out of cyber-physical attacks, the relevant policy language may not be sufficiently explicit to preclude protracted and costly coverage litigation.

Therefore, unless and until policy language and case-law catch up with the risk, it is important for policyholders—especially those most at risk of a catastrophic cyber-physical attack, such as those in the shipping or transportation industries—to review their potentially relevant policies, determine what coverages those policies do (and arguably do not) in fact provide, and fill in any gaps (or potential gaps) promptly.

A "cyber-physical attack," according to the International Risk Management Institute, Inc.'s online glossary, is "a security breach in cyber space that impacts on the physical environment. A malicious user can take control of the computing or communication component of water pumps, transportation, pipeline valves, etc. and cause damage to property and put lives at risk."

For example, Gallagher, which provides insurance, risk management and consulting services, states:

"Consider the onset of positive train control (PTC) in the rail industry. PTC is a system of functional requirements for monitoring and controlling train movements—the goal is to improve the safety of train traffic by only permitting movement if there is a positive permission, and in the absence of that positive permission the movement is halted. This system has been designed to prevent rail collisions but a cyber-attack could cause the system to fail resulting in property damage to the train and surrounding infrastructure, with bodily injury to passengers and others nearby."

Gallagher continues:

"This use and reliance on operational technologies exists in many other areas of our economy too—including manufacturing, utilizes (power, water, etc.) heavy industry and critical infrastructure. Supervisory control and data acquisition (SCADA) systems and other industrial control systems (ICS) are used to monitor and control key processes related to electrical power grids, water distribution, wastewater collection systems, oil and LNG pipelines, railway transportation systems, manufacturing plants and refineries.

Consider also the marine shipping industry: In 2014, Business Insurance reported that "maritime companies face significant cyber threats as they adapt their navigational, operational and other equipment to the digital world." Today, more and more large vessels are automated, or at least rely on automated processes, such as global positioning systems (GPS), automatic identification systems (AIS) and electronic chart displays and Information Systems (ECDIS). If an attacker is able to hack into and/or take control of a ship's GPS, AIS or ECDIS system(s), a serious accident resulting in bodily injury could occur.

Citing the then-vice president of cyber security and privacy at Lockton Cos. Business Insurance observed that "cyber risks no longer are just about privacy and personal information." Four years later, in April 2018, Reuters reported, "Cyber-physical risk will only increase as more machines, from medical devices to fuel tankers, become connected to the 'Internet of Things.'" Addressing the 2020 RSA conference, Mary T Barra, chairman and chief executive officer of General Motors Co., observed, according to Infosecurity Magazine, "'that there are virtually no industries today that are not vulnerable to cyber-attacks.'" Ms. Barra reportedly noted "that the auto industry is no exception."

These risks are far from theoretical. For example, in 2008, a teenager hacked into the Lodz, Poland, tram system. That "prank," according to Wired, "derailed four trams and injured a dozen people." At least one power plant and one steel mill also have been targets of cyber-physical attacks. While those latter attacks seem to have resulted only in physical property damage, the outcomes could have been much worse.

When a cyber-physical attack causing bodily injury does occur, an injured party may assert a claim against the business that was hacked or attacked. While many policyholders may simply assume that such claims would be covered by their all-risk marine, CGL, or traditional cyber liability insurance policies, policy language may dictate a different outcome, or, at least, insurance companies may argue otherwise.

Marine hull and cargo insurance policies, for example, often include an "Institute Cyber Attack Exclusion Clause (CL 380) (10/11/2003)." That exclusion to coverage provides, with limited exception, that "in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operations, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process of any other electronic system."

Further, according to Reuters, "over time, exclusions and lower sub-limits have crept into traditional [CGL] policies that can leave many insureds with little or no coverage for cyber-induced physical losses, including losses that would have been fully covered had they not been induced by hacking." "CGL policies," that report continues. typically contain one of two ISO endorsements (revised in 2014) that stingy insurers could interpret to exclude cyber-physical risk."

One common CGL exclusion negates coverage for "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." And, as the Reuters report points out, "'electronic data' is defined to include not only information, but also software and computer programs Thus, insurers could argue that the language excludes property damage and/or bodily injury claims arising from a wide range of malicious hacking activities, and not just the theft of private information."

Conversely, traditional cyber policies often exclude coverage for claims involving bodily injury. One exclusion often found in such policies negates coverage for any "loss (including costs of defense): … based upon or arising out of any claim for … bodily injury or property damage, except for bodily injury arising exclusively out of emotional distress allegedly caused by" certain wrongful acts, which generally would not be at issue in such circumstances.

Combined, these various exclusions leave a notable, and dangerous, gap in coverage. Marsh, for one, identified this gap back in 2014. In a report titled, "Cyber Gap Insurance—Cyber Risk: Filling the Coverage Gap," that broker identified "the gaps in coverage created by [such] exclusions" and noted that those gaps "potentially leave catastrophic events unindemnifiable."

For example, imagine a scenario in which a large ship's (or train's or self-driving car's) navigational system is hacked, causing that ship (or train or car) to run into another vessel (or train, car, etc.), killing passengers onboard the second ship (or train, car, etc.). If the large ship's owner is thereafter sued by the families of the deceased passengers, the owner in turn would likely seek insurance coverage. However, the owner may be denied coverage under a typical all-risk marine policy, or even perhaps under a typical CGL policy. An insurer may contend that the damage was caused by a computer, and the injury arose out of damage to certain of the ship's computer programs. At the same time, the owner also may be denied coverage under a traditional cyber policy because the third-party claim involves a bodily injury.

Although this potential gap was identified years ago, the insurance industry has been slow to fill it. A review of insurers' public websites and marketing materials reveals that few insurers purport to offer cyber insurance intended to clearly cover third-party liability claims involving bodily injury. AIG, though, at least represents that its "CyberEdge Plus" coverage "covers losses in the physical world caused by a cyber event, including primary coverage for business interruption, first and third party property damage, physical injury

to third parties and products/completed operations coverage." Of course, the "devil is in the details," and a policyholder should carefully review any specimen policy forms purporting to offer to such coverage prior to placement.

While policyholders may already be entitled to such coverage under existing forms, insurance policies that clearly delineate coverage for bodily injuries caused by cyber-physical attacks would remove uncertainty. In the absence of such forms, a policyholder should carefully review at least its current liability and cyber policies to determine what coverages and gaps may exist. If there is any question or ambiguity about whether a policyholder has the requisite coverage, it should take appropriate steps to resolve that doubt and fill the gap. To do so, it may need to purchase an additional insurance policy or endorse an existing policy to make clear that it covers the risk in question. Policyholders should be proactive and not leave coverage to chance. The risk is too great.

Michael H. Sampson *is a partner with Leech Tishman and a member of the firm's litigation practice group. He is also chair of the firm's insurance coverage group, co-chair of its cannabis group and a member of the data privacy and cybersecurity group. Based in the Pittsburgh office, Sampson represents diverse clients in a variety of complex civil and commercial litigation and other matters across the country.*
