COVINGTON

Cyber-Physical Risks: Are You Covered?

December 14, 2016

Insurance Recovery and Cybersecurity

Recent reports from both government and private groups have highlighted the risk that cyber hacking may now cause serious physical injury or damage. This new risk stems from connected industrial controls or electronic devices comprising the Internet of Things (IoT)—the network of over 50 billion objects ranging from children's toys to home appliances to medical devices to critical infrastructure components. With such physical risk comes potential liability for those who make or use these networked products.

But does insurance cover this novel liability risk? This alert discusses potential coverage issues for claims alleging physical harm from cybersecurity failures. It also offers practical tips to address these emerging risks and the insurance issues surrounding them.

Cyber-Physical Risks

The December 1 final report from the President's blue-ribbon Commission on Enhancing National Cybersecurity warns that "as the computing power in connected devices increases—and as we come to depend on them to control, either directly or indirectly, machinery with the power to create kinetic effects (whether electrical or mechanical)—the dangers will increase dramatically." Similar warnings from the National Institute of Standards and Technology (NIST) appear in its recent cybersecurity guidelines for IoT products. And for a computer security conference on the IoT this month, an international team of researchers issued a report finding potentially fatal hacking vulnerabilities in 10 different types of medical implants.

These recent reports follow on highly publicized hacks targeting networked infrastructure, household appliances, or other "things" instead of conventional computer networks. These novel cybersecurity vulnerabilities arise courtesy of what NIST refers to as "cyber-physical systems": interacting networks of physical and computational components, including smart grids and "smart" anything else, such as cars, hospitals, homes, or appliances. Hackers of these systems have remotely derailed trains, pumped raw sewage onto public and private property, modified HVAC systems in hospitals with vulnerable patients, disabled oil pipeline leak-detection systems and nuclear power plant safety monitoring systems, and caused widespread power outages. In sum, the threat from compromised "smart" devices is not confined to data theft or web service disruptions (such as the recent "Mirai botnet" attacks launched from "smart" security cameras). They can cause actual physical harm.

An ever-wider range of policyholders may be exposed to liability for these cyber-physical risks, including companies that manufacture or use networked or IoT-connected products. Indeed, the President's Commission specifically proposed an assessment of "the current state of the law with regard to liability for harm caused by faulty IoT devices," in part to "provide appropriate incentives for companies to design security into their products."

Liability Insurance for Cyber-Physical Risks

Despite wider recognition of these physical risks from cyber perils and accompanying liability risks, cyber insurance buyers are finding that the available cyber forms typically *exclude* bodily injury and property damage. These exclusions are ostensibly intended to prevent cyber policies from duplicating the coverage traditionally afforded by general liability policies.

But do those more conventional policies cover physical harm when it arises from a cyber-related peril? Policyholders would normally look to their Commercial General Liability (CGL) policies to cover claims alleging bodily injury or property damage. But since 2014, most CGL policies contain two types of cyber-related exclusions for physical damage to tangible property or bodily injury:

- damages arising out of "[t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data"; and
- damages arising out of "[a]ny access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information."[1]

On their faces, these exclusions appear to aim solely at data breaches of private or protected information, and the regulatory submissions from insurers seeking approval for them focused on that risk. But the wording of these exclusions is sufficiently broad and unclear that an aggressive insurer might argue, for example, that a hacker overwriting the instructions for an industrial control system to damage factory machinery constitutes "damage to" or "corruption of" data; or that bodily injury caused by alteration of a patient's dialysis machine settings arose out of "access to . . . any person's health information or any other type of nonpublic information," thus excluding liability coverage for the hospital or medical device manufacturer.

Policyholders have good arguments, from both the text and drafting history of the policies, that these exclusions should not be stretched to exclude all traditional bodily injury and physical damage caused by hacking.[2] Ultimately, however, the question of coverage for such attacks may be fact-intensive and dependent upon a careful analysis of how each harm arose.

Lessons for Policyholders

Policyholders (and insurers) are confronting a relatively novel set of risks: old-fashioned physical harms arising from modern cyber perils. To address these new risks, policyholders should consider the following steps:

---

[1] *See* Insurance Services Office, Inc., *Commercial General Liability Coverage Form, CG 00 01 04 13* § I.A.2.p, at 5; Insurance Services Office, Inc., *Exclusion—Access or Disclosure of Confidential or Personal Information and Data-Related Liability—With Limited Bodily Injury Exception, CG 21 06 05 14*; Insurance Services Office, Inc., *Exclusion—Access or Disclosure of Confidential or Personal Information and Data-Related Liability—Limited Bodily Injury Exception Not Included, CG 21 07 05 14*.

[2] *See* John Buchanan & Dustin Cho, "When Things Get Hacked: Coverage for Cyber-Physical Risks," at 6–9, *ABA Litigation Section, Insurance Coverage Litigation Committee* (Mar. 3, 2016).

- *Understand the cyber-physical risks.* This means surveying the industrial control systems and other networked "smart" devices that the policyholder either manufactures or uses in its own operations; hardening their cybersecurity; and analyzing the potential consequences if a hacker should get past those cybersecurity defenses.
- *Analyze how all policy language will respond to those risks.* This means scrutinizing the policy terms under cyber, general liability, first-party property, and any other potentially applicable lines of coverage, such as crime, E&O and D&O. Do the "dovetailing" exclusions actually dovetail? Or do they leave gaps—whether because they contemplate protection from another line of coverage that in fact has a reciprocal exclusion, or merely because one policy's coverage wording does not align intelligently with another policy's exclusion wording?
- *If possible, plug the gaps and clarify the coverage grants.* Some insurance buyers may be able to negotiate changes in their existing policies that clarify coverage specifically for cyber-physical risks. Others may need to explore the purchase of new specialty insurance solutions, such as difference-in-conditions excess coverage.
- *Expect disputes.* Claims disputes are common with any previously unrecognized or underestimated risk. But attention to both the big picture and the nitty-gritty details at the underwriting stage may reduce the chances that cyber-physical losses will result in coverage litigation at the claims stage.

Policyholder counsel at Covington can help our clients spot defects and gaps in their coverage—before they purchase it—and devise strategies to align their policy wordings more closely with their potential cyber exposures. In guiding our clients through the still uncharted waters of the cyber insurance underwriting process, we bring the experience gained from handling some of the largest data breach coverage claims in history. We also draw upon the expertise of our counterparts in the firm's Data Privacy and Cybersecurity group, who advise clients daily how to prevent and respond to cyber incidents of all kinds.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Insurance Recovery practice group:

John Buchanan	+1 202 662 5366	jbuchanan@cov.com
Dustin Cho	+1 202 662 5458	dcho@cov.com