When Things Get Hacked: Insurance Coverage for IoT-Related Risks

John Buchanan and Dustin Cho

I. Introduction

Hackers can do more than steal your data. When they access IoT-connected things—whether household appliances, smart wearables, medical devices, industrial control systems, smart grids, or smart cities—hackers and other bad actors can damage property and endanger lives. As one commentator has put it, “American officials are discovering that in a world in which almost everything is connected—phones, cars, electrical grids, and satellites—everything can be disrupted, if not destroyed.”

Reports in recent years highlight some disturbing threat scenarios. Russian government cyber actors have reportedly gained remote access to networks capable of disrupting critical U.S. infrastructure, including the energy sector and the power grid. Cyber soldiers sitting behind...

1. This paper is adapted from Chapter 17 of Internet of Things (IoT): Legal, Policy, and Practical Strategies, a forthcoming ABA publication scheduled for release at the Science & Technology (SciTech) Section’s Internet of Things (IoT) National Institute on March 27, 2019.

2. The authors are lawyers in the Washington, D.C. office of Covington & Burling LLP, who represent policyholders exclusively in coverage litigation. The opinions stated in this chapter are those of the authors and should not be attributed either to their law firm or to its clients.


(continued…)

DC: 6916992-6
computers in Tehran could open the floodgates on a suburban Westchester County dam.\textsuperscript{5} Or the threat could be as banal and close to home as bored teenagers down the street hijacking your “smart” home appliances,\textsuperscript{6} or, more ominously, the city’s trolley system.\textsuperscript{7}

These novel threats arise from what the National Institute of Standards and Technology refers to as “cyber-physical” or “smart” systems, that is, the “co-engineered interacting networks of physical and computational components” that allow the real world and digital world to interact in unprecedented ways.\textsuperscript{8} Unfortunately, the cyber-security defenses in many “smart” IoT-connected systems are often . . . not too smart. Hence the reports of hacks on a wide variety of networked IoT devices ranging from smart toilets\textsuperscript{9} to drones\textsuperscript{10} to medical devices.\textsuperscript{11} The federal government’s alerts and subsequent security briefings in 2018\textsuperscript{12} have raised the general level of awareness of potentially massive physical losses from hacking the IoT or industrial IoT, including attacks on power grids or other networked critical infrastructure.


\textsuperscript{9} See Hill, supra note 6.


\textsuperscript{12} DHS-FBI Alert, supra note 4; Awareness Briefings: Russian Activity Against Critical Infrastructure, Nat’l Cybersecurity & Commc’n’s Integration Ctr (NCCIC), https://share.dhs.gov/p344qjbhqu03/.

(continued…)
These increased warnings of the risk of massive physical losses from cyberattacks naturally raise the question whether that risk can be mitigated by insurance. In fact, a 2015 report titled “Business Blackout,” prepared by Lloyd’s and Cambridge University, anticipated the types of IoT-related attacks on critical infrastructure that have been the subject of the 2018 federal government warnings, and it analyzed what insurance implications might flow from them.\(^\text{13}\) Specifically, the report hypothesized a (now all too plausible) scenario, in which a cyberattack on a utility’s industrial control systems disables or destroys multiple power generators in a “smart” grid, resulting in cascading losses throughout the blacked-out power grid and beyond.\(^\text{14}\) Such losses could include first-party physical property damage and business-interruption loss for utilities and their customers, third-party property damage and bodily injuries arising from the grid shutdown, and even looting and other social unrest, with accompanying liabilities for the businesses affected.\(^\text{15}\)

The cyber insurance market hasexploded in recent years; dozens of insurers now offer some kind of cyber coverage.\(^\text{16}\) Most cyber-related policies address the intangible losses that accompany network intrusions and data hacks—with a particular focus on privacy-related losses.\(^\text{17}\) Thus, while coverage is subject, as always, to the specific (and widely variable)


\(^{14}\) Id. at 11–13.

\(^{15}\) Id. at 16–19.


(continued…)
wordings of these nonstandard policy forms, if an attack on IoT-connected devices involves
conventional data privacy losses, then most available cyber policies can be expected to provide
some protection.

But insurance protection for so called cyber-physical risk—the physical losses that may
result from the cyber peril of an IoT-related attack—presents a more complex question under
many commonly available insurance policies. In fact, most off-the-shelf cyber forms expressly
exclude coverage for physical bodily injury and property damage.¹⁸ Originally, insurers drafted
such exclusions to prevent cyber policies from duplicating the coverage traditionally afforded by
standard-form commercial general liability (CGL) and first-party property policies.¹⁹

But do conventional liability and property policies still clearly cover bodily injury or
property damage when it arises from a cyberattack involving IoT devices? This chapter analyzes
coverage issues that may arise under traditional CGL and property policies where cyber-physical
risks are involved, including the arguments that insurers may raise to escape coverage under such
policies and the arguments that policyholders may raise in rebuttal. It then discusses examples of
the specialty insurance products that have started to emerge to provide coverage (at a price) for
physical harms from cyber perils. It concludes with a few general observations and
recommendations for insuring IoT-related risks.

¹⁸ See id. at 72–75, 88–90 (charting the availability both of first-party coverage for direct damage to
equipment and of third-party coverage for bodily injury and property damage).

¹⁹ See infra note 20.

(continued…)
II. Commercial General Liability Insurance Coverage for Bodily Injury or Property Damage Caused by Cyber Attacks through the IoT

Cyber insurance is now widely available; but as stated above, most cyber policies currently exclude third-party liability coverage for bodily injury and property damage. The explanation commonly provided for this exclusion is that “such losses are covered under CGL . . . policies.” But in fact, most recent standard-form CGL policies now incorporate their own cyber-related exclusions—the scope of which is not always clear. This section discusses the evolution of those exclusions and the coverage issues they present in the context of IoT risks.

A. Cyber Exclusions in the CGL Form

Since the turn of this century, the Insurance Services Office (ISO) has repeatedly revised the standard CGL policy’s bodily injury and property damage liability coverage part (titled “Coverage A”) with respect to cyber-related risks. First, in 2001, the standard CGL policy was revised to state that damage to electronically stored data would not be considered damage to tangible property. Next, in 2004, it was revised to exclude “[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic

20. Robert Bregman, Cyber and Privacy Insurance Coverage, 37(11) IRMI, THE RISK REPORT 1 (July 2015), (“The [cyber] policies exclude claims alleging bodily injury and property damage because such losses are covered under CGL/property insurance policies.”).

21. The 2001 Insurance Services Office CGL policy form added the following two sentences to the definition of “property damage”:

For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

In this form “property damage” is defined as “[p]hysical injury to tangible property, including resulting loss of use of that property,” and “[l]oss of use of tangible property that is not physically injured.” See ISO Properties, Inc., Commercial General Liability Coverage Form, CG 00 01 10 01 § V.17, at 15 (2000).

(continued…)
According to ISO, this new exclusion, “Exclusion p,” removed coverage for damage to physical property caused by loss of electronic data.\textsuperscript{22} In 2013, a sentence was added to Exclusion p that carved out from the exclusion any “liability for damages because of ‘bodily injury.’”\textsuperscript{23} That is to say, the new sentence expressly \textit{preserved} coverage for bodily injury arising out of the loss of electronic data.

In May 2014, ISO published two versions of an endorsement that revises Exclusion p: one with a “limited bodily injury exception” and one without.\textsuperscript{24} The latter endorsement, in part, reverts to the 2004 variant of Exclusion p—it excludes any damages arising out of the loss of electronic data, regardless of whether the damages are because of bodily injury or property damage.\textsuperscript{25} The version with a “limited bodily injury exception” in part adheres to the 2013 edition of Exclusion p, which preserves coverage for damages because of bodily injury.\textsuperscript{26}

\textsuperscript{22} See ISO Properties, Inc., \textit{Commercial General Liability Coverage Form, CG 00 01 12 04} § I.A.2.p, at 5 (2003). The definition of “electronic data” used in this exclusion was the same as the definition of “electronic data” that the 2001 standard CGL policy had introduced in its definition of “property damage.”


\textsuperscript{24} ISO also published a third version that applies only to Coverage B, the coverage for “personal and advertising injury liability” (thus omitting the revisions to Exclusion p in Coverage A). See Insurance Services Office, Inc., \textit{Exclusion—Access or Disclosure of Confidential or Personal Information (Coverage B Only), CG 21 08 05 14} (2013).

\textsuperscript{25} The “limited bodily injury exception not included” endorsement states in relevant part:

This insurance does not apply to: . . . Damages arising out of: (1) Any 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; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

Insurance Services Office, Inc., \textit{Exclusion—Access or Disclosure of Confidential or Personal Information and Data-Related Liability—Limited Bodily Injury Exception Not Included, CG 21 07 05 14} (2013).

\textsuperscript{26} The “limited bodily injury exception” endorsement states in relevant part:

This insurance does not apply to: . . . Damages arising out of: (1) Any 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 (continued…)}

What was new and identical in both 2014 endorsements was the addition of paragraph (1) of Exclusion p—an exclusion for all damages (whether because of bodily injury or not) 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.”

In isolation, the undefined terms “access to” and “nonpublic information” are sufficiently vague that an aggressive insurer might argue, for example, that a hospital’s or medical device manufacturer’s liability for bodily injury caused by alteration of a patient’s dialysis machine settings would constitute excluded damages because they arose out of “access to . . . any person’s health information or any other type of nonpublic information”; or similarly, that liability for property damage or personal injuries resulting from a hacker’s manipulation of the data regulating industrial control systems in a nuclear plant or power grid arose from “access to . . . nonpublic information” and thus is excluded.

In response, insureds would argue that this exclusion, read within its context, cannot reasonably encompass all traditional bodily injury and physical damage caused by hacking of industrial control systems, malicious or negligent alteration of medical device settings, or other

---

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 (2013).

27. See notes 25 and 26.
types of access to nonpublic electronic data regulating networked “things” through the IoT, for at least the following reasons:

- **“Nonpublic Information.”** The settings and controls of devices and machinery, though not necessarily accessible to the “public,” are not reasonably construed as “any other type of nonpublic information” as contemplated by the exclusion. The interpretive canon of *ejusdem generis* instructs that when a series of items in a list share a certain core characteristic, a “catch-all” term at the end of the list should not be read to stretch beyond what the specifically listed items have in common. In these endorsements, the specifically listed types of “nonpublic information” preceding the catch-all phrase are all traditionally confidential information whose confidentiality is recognized, and protected, by law.

Networked device settings and machine instructions do not generally enjoy either legal or popular recognition as inherently private information. Such data are qualitatively different from the specific categories of protected information listed in paragraph (1) of Exclusion p: “trade secrets, processing methods, customer lists, financial information, credit card information, [and] health information.” Under this interpretive principle, therefore, the catch-all term “and any other nonpublic information” in the exclusion endorsements would be read to include other categories of information whose confidentiality is recognized under and protected by the law; but it would not be stretched to encompass a qualitatively different type of “information”—the data regulating electronic control systems.

---


29. The exclusion’s list of various types of “confidential information” arguably starts after the first term, “patents.” While patents are publicly disclosed once granted, they share legal protections similar to those enjoyed by other enumerated types of information such as “trade secrets.”
Reinforcing this reading, both endorsements specifically list examples of the damages to which the exclusion applies—all of which are damages associated specifically with data privacy breaches:

This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of that which is described in Paragraph (1) or (2) above.\(^{30}\)

All of these types of expense relate to common responses to data breaches, and indeed it is difficult to conceive how the first two items in the list—notification costs and credit monitoring expenses—could arise in the event of traditional physical bodily injury or property damage. This clause’s focus on privacy-breach damages reinforces the conclusion that the exclusion was intended only for privacy-related liabilities and not for physical harm that happens to have resulted from a malfunctioning electronic device.

- **“Access To.”** Although manipulation of a machine’s or device’s settings may involve “access to” those settings, the scenarios of concern do not “aris[e] out of” the access to the data that comprises those settings (much less their “disclosure” to the public). Rather, they arise out of the overwriting or overriding of that data—whether intentionally (through hacking) or unintentionally (through user error or a programming bug). In context, damages “arising out of . . . [a]ny access to or disclosure of . . . nonpublic information” means damages arising out of obtaining nonpublic information—the damages that typically arise from privacy breaches. When the hacking of industrial control systems or networked devices results in physical harm, by

\(^{30}\) 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 (2013); 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 (2013).
contrast, the cause is not the *obtaining* of nonpublic information: that is, the prior, correct settings for the machinery or devices in question. Rather, it is the introduction of new instructions that override the original settings. For example, a hacker could alter a dialysis machine’s settings even if he could not read the “information” in those settings before he overwrote them. Likewise, a hacker could disrupt a digital signal that provides instructions to a networked device without necessarily receiving or decoding the original intended signal.

In other words, the types of hacking that affect the operations of networked devices do not typically arise out of accessing any *information*—what the exclusion requires. Instead, they arise from someone’s access to the *system or location* where the information is stored. What causes the harm is the new, erroneous digital settings or instructions that replace the original settings or instructions. Whether or not those original, correct settings are considered “nonpublic information,” the intruder’s access to that information is beside the point: the harm arises from the newly introduced malicious information, not from access to the “nonpublic information” itself. Unless the insurer can provide compelling forensic evidence that the essential cause of physical loss was the *release* rather than the *alteration* of confidential information in device settings, the exclusion should not apply.31

31 The insurance industry’s contemporaneous explanations of Exclusion p are also consistent with a reading that confines the exclusion to data-related, not physical, harm. The memorandum that ISO submitted to regulators in 2013 explaining its adoption of these endorsements states that “damages related to data breaches, and certain data-related liability, are not intended to be covered under the abovementioned coverage part. These types of damages may be more appropriately covered under certain stand-alone policies including, for instance, an information security protection policy or a cyber liability policy.” Insurance Services Offices, Inc., *Access or Disclosure of Confidential or Personal Information Exclusions Introduced*, Commercial Lines Forms Filing CL-2013-ODBFR, at 7, 8 (2013) (on file with authors) (emphasis added). ISO’s statement is consistent with an ISO executive’s explanation of the endorsements shortly after they were introduced: he identified other “standalone” ISO insurance products that were available “to provide certain coverage with respect to data breach and access to or disclosure of confidential or personal information,” thus suggesting that the new exclusions were intended to dovetail with cyber policies. See ISO Comments on CGL Endorsements for Data Breach Liability Exclusions, Ins. J. (July 18, 2014), available at http://www.insurancejournal.com/news/east/2014/07/18/332655.htm (quoting Ron Biederman, assistant (continued…)}

Paragraph (2) of Exclusion p uses the same language used in CGL policies since 2004 to exclude 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.” As noted earlier, since 2014 this exclusion comes in two different versions. The “limited bodily injury exception” version, like the 2013 standard CGL policy, expressly preserves coverage for bodily injury. The other version, like the 2004 standard CGL policy, contains no express carve-out for bodily injury. In both formulations, as with paragraph (1), insurers would likely face a difficult burden to prove that this paragraph (2) exclusion applies to the most common source of cyber-physical loss: physical harms arising from IoT hackers overwriting or overriding the controls of electronic devices.

In sum, Exclusion p in the standard CGL form appears to be aimed at the privacy risks covered under separate cyber policies. But its uncertain application in the context of IoT-related cyber-physical harm may well give rise to highly technical—and no doubt costly—coverage disputes, with the insurer bearing the burden of proving that this exclusion precludes coverage for harm from an IoT attack.

---

32. 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 (2013); 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 (2013). (continued…)
III. First-Party Property Coverage

Many first-party property policies do not explicitly address coverage for physical harm from a cyberattack.\textsuperscript{33} Some, like the ISO’s standard “all risks” and “named perils” policies, may not mention cyber-related risks at all in their cause of loss forms.\textsuperscript{34} Others may include cyber exclusions targeting only harm to intangible property.

If such a “cyber-silent” policy is an “all risks” policy, meaning it covers losses unless caused by a specifically excluded peril, then coverage for physical damage from a cyberattack should presumptively exist. As one commentator has observed, however, some in the insurance industry assert that standard all risks policies were not created with cyber perils in mind.\textsuperscript{35} But an insurer’s failure to anticipate a novel risk should not negate the core function of an “all risks” policy; it promises coverage unless an exclusion applies.\textsuperscript{36} Without a cyber-specific exclusion to rely on, an insurer facing a claim for physical losses from a cyberattack would likely have to show that the attack fits within some non-cyber-specific exclusion to justify denying coverage.

If a cyber-silent policy is written on a “named perils” basis—meaning it covers only harms from expressly enumerated risks—coverage could still be found in many cases. Under the standard ISO policies, and most others, cyberattacks, as such, are not named perils. Still, they may sometimes fall within the scope of a named peril’s definition. For example, the ISO policies

\textsuperscript{33} See Lloyd’s Emerging Risk Report, \textit{supra} note 13, at 37.
\textsuperscript{35} See Alex Lathrop, \textit{Does Traditional Coverage Apply When Cyber Attacks Cause Physical Damage?}, PROPERTY CASUALTY 360, at 3 (Dec. 29, 2016, 3:00 AM), \url{http://www.propertycasualty360.com/2016/12/29/does-traditional-coverage-apply-when-cyber-attacks?slreturn=1515084401&page=3}.
\textsuperscript{36} See id. (continued…)
name “vandalism” as a covered risk and define it as “willful and malicious damage to, or destruction of,” insured property. To be sure, some insurers may balk at coverage under such a provision, asserting that what they meant to cover was only the traditional forms of vandalism, like a brick through a window, not cyber-related perils. But the “vandalism” definition is silent on means and relates only to intent—and many IoT hackers “willfully” or “maliciously” destroy insured property.

Even if a cyberattack does not fit within a named peril’s definition, it may result in such a peril—for example, a fire or explosion. In cases where hacking either counts as a named peril or creates such a peril, an insurer would again need to point to a non-cyber exclusion to justify a denial of coverage. This potential exposure to the risk of cyber-physical damage under garden-variety property policies and other traditional policies has been characterized as the “silent cyber risk” that many insurers must evaluate more carefully.

Although many property policies are still silent on cyber risks, some insurers are attempting to exclude them through endorsements or otherwise. For instance, one London Market form common to energy, marine, and industrial property policies, the Institute Cyber Attack Exclusion (CL 380), excludes from coverage any damage “arising from the use or

37. See Alex Lathrop & Janine Stanisz, Hackers Are After More Just Data: Will Your Company’s Property Policies Respond When Cyber Attacks Cause Physical Damage and Shut Down Operations?, 28 ENVTL. CL. J. 286 (2016) (raising the possibility that an attack might count as “vandalism” and analyzing coverage for physical damage from multiple, hypothetical cyberattacks under both all risks and named perils policies).


(continued…)
operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.”  

Another London Market form, LMA 3030, excludes from property terrorism insurance “[l]oss or damage by electronic means including but not limited to computer hacking or the introduction of any form of computer virus or corrupting or unauthorised instructions or code or the use of any electromagnetic weapon.” These exclusions remain untested in the courts; whether one of them would preclude coverage for the particular circumstances of any given IoT hack may both raise subtle interpretive questions and require a fact-intensive technical analysis.

As new, nonstandard policy wordings proliferate to address the emerging risk of physical property damage from hacking of networked devices, first-party property insurance buyers will increasingly need sharp eyes, and sophisticated coverage advice, to evaluate what protection their policies provide.

IV. Emerging Coverage Solutions

Given the potential for coverage disputes under traditional CGL and property policies, as well as the growing potential for cyber-physical exposures from IoT-connected things, many policyholders may seek purpose-built coverage for risks of physical harm from cyber perils. The market for such products, like the threats they cover, is still evolving. A 2018 market survey of


(continued…)
cyber insurance products indicates that such coverage options are still confined to a relative
handful of insurers.41

Nonetheless, the number of insurance products that explicitly cover physical damage
from cyber risks can be expected to grow steadily over the next several years. Some signs are
already pointing in this direction. As reported in the insurance trade press, FM Global has
reported increased inquiries about its products offering cyber-physical coverage;42 AIG
announced in 2017 that it would include cyber coverage in its commercial casualty policies—a
move that would likely eliminate Exclusion p and the accompanying coverage issues discussed
earlier;43 and Chubb has introduced an endorsement to address, in part, uncertainty over what
happens when a cyber incident creates damage traditionally covered under a property policy.44 In
the United Kingdom, meanwhile, the government-backed terrorism reinsurer, Pool Re,
announced in 2017 that it would offer coverage for physical damage from cyberterrorism,
following a report on the issue that it produced with the University of Cambridge’s Judge

41. See Betterley, supra note 17, at 88–90 (“Third-party Coverage: Bodily Injury and Property Damage”
summary chart).

42. See Katie Dwyer, Cyberattacks Reach the Physical Realm, RISK & INSURANCE (July 27, 2017),

43. See, e.g., Suzanne Barlyn, AIG to Include Cyber Coverage to Commercial Casualty Insurance, REUTERS
casualty-insurance-idUSKBN1CV2XE.

44. Judy Greenwald, 2017 Innovation Awards: Chubb Global Cyber Facility and Property and Casualty
Endorsements, BUS. INS. (Oct. 2, 2017),
http://www.businessinsurance.com/article/00010101/NEWS06/912316218/2017-Innovation-Awards-Chubb-Global-
Cyber-Facility-and-Property-and-Casualty-En (quoting a Chubb executive as saying, “There are questions, for
instance, as to what happens if a cyber incident leads to damage covered by traditional property policies. . . . We
don’t want uncertainty for our clients.”).

(continued…)
Business School. This reinsurance protection may motivate commercial insurers to offer coverage for cyber-physical risks that they may currently attempt to exclude.

These market developments are too numerous, and too fluid, to warrant a comprehensive survey that could become obsolete within a matter of months. But one relatively recent insurance product offers a glimpse into where the market may be heading in response to these novel risks. Global insurance broker Marsh has developed a broad proprietary policy wording, known as Cyber CAT 3.0, crafted to maximize coverage across a range of insurance coverage lines for evolving cyber risks. Cyber CAT 3.0 is specifically promoted as providing “Internet of Things coverage for negligence in the design or manufacture of an IoT product and/or service,” as well as coverage for “[p]roperty damage to tangible property caused by a cyber event” and “[b]odily injury and property damage liability resulting from a cyber event.”

Policyholders desiring greater contract certainty around cyber-physical risks should consider carefully these new policies and endorsements. Some, like the Marsh form, show promise to prevent the potential coverage disputes identified in this chapter. Over the next decade, as the risk of cyber-physical harm grows more salient, more and more specialty insurance products can be expected to respond to rising market demand for more secure protection against such harms.


47. Id. at 2.
V. Conclusions and Recommendations for Entities with IoT Risk Exposures

Both insurers and insureds are confronting a relatively novel set of risks: old-fashioned physical harms arising from newfangled cyber perils. Many insureds confronted with these cyber-physical losses will argue that they should be covered under their conventional all-risk general liability and first-party property policies. Some insurer-side claims handlers may look for reasons why these risks should fall outside the policy terms.

To address these new issues, insurance purchasers would be well advised to take the following steps:

- **Understand the cyber-physical risks involved.** This means surveying the industrial control systems and other networked “smart” devices that the insured either manufactures or uses in its own operations; hardening the cybersecurity of those systems and devices; and thinking through the potential consequences of a cybersecurity failure.

- **Understand how all policy language will respond to those risks.** This means at a minimum analyzing the policy terms under cyber, technology errors and omissions, general liability, property and any other potentially applicable lines of coverage, such as kidnap and ransom policies and even directors and officers policies. 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 the coverage grant in one line fails to align intelligently with the exclusion in another?

- **If possible, plug the gaps and clarify the coverage grants.** To clarify coverage specifically for cyber-physical risks, insurance buyers may request changes in their existing lines of coverage or explore the purchase of specialty coverage solutions.
• **Expect disputes.** They are virtually inevitable at the claims stage with any previously unrecognized or underestimated risk. But attention to both the big picture and the nitty-gritty details at the underwriting stage should reduce the chances that IoT-related risks and cyber-physical losses will generate the next big wave of coverage litigation.