Originally Presented at the ABA Litigation Section, Insurance Coverage Litigation Committee
Hack That Thing: Physical Harms from Cyber Perils — Are They Covered?
Tucson, Arizona — March 3, 2016

When Things Get Hacked: Coverage for Cyber-Physical Risks

John Buchanan & Dustin Cho[1]

Hardly a day goes by lately without a headline about some new and previously unheard of cyber hack — involving not a conventional computer network, but rather some industrial machine or household appliance, or even a child's toy. These novel cybersecurity vulnerabilities arise courtesy of what the National Institute of Standards and Technology ("NIST") refers to as cyber-physical systems or "CPS": "co-engineered interacting networks of physical and computational components."[2] As NIST further explains:

> "Other phrases that you might hear when discussing these and related CPS technologies include:
> – Internet of Things (IoT)
> – Industrial Internet
> – Smart Cities
> – Smart Grid
> – 'Smart' Anything (e.g., Cars, Buildings, Homes, Manufacturing, Hospitals, Appliances)."[3]

The problem with many of these "smart" things is that — for a variety of reasons, many of them admirable — their protections against unauthorized electronic access are not so smart. Hence the steady stream of reports about novel cyber hacks involving networked things. For example:

---

[1] John Buchanan is a partner and Dustin Cho is an associate in the Washington, D.C. office of Covington & Burling LLP. The authors represent policyholders exclusively in coverage litigation. The opinions stated in this paper are those of the authors and should not be attributed either to their law firm or to its clients.

[2] Nat'l Institute of Standards and Technology, Cyber-Physical Systems Homepage, http://www.nist.gov/cps/ (Feb. 18, 2016).

[3] *Id.*

- WiFi remote-controlled toy drones,[4] and more ominously, both commercial and military drones[5];
- "smart" household appliances, including "smart" toilets[6];
- electronically-controlled functions in a Jeep — including its transmission[7]; and
- medical devices, including insulin pumps and pacemakers.[8]

A recent report titled "Business Blackout," prepared by Lloyd's and the University of Cambridge, hypothesized a cyber-physical hack with far more devastating consequences: one that brings down an entire "smart" power grid.[9] In this imaginary (but far too plausible) "Business Blackout" scenario, a cyber attack on a utility's industrial control systems disables or destroys multiple power generators, resulting in cascading losses throughout the blacked-out power grid and beyond.[10] These losses include not only first-party physical property damage and time-element loss for utilities and the customers who depend on them, but also third-party property damage and bodily injuries arising from the grid shut-down, and even looting and other social unrest, with accompanying liabilities for many of the businesses concerned.[11]

Meanwhile, in recent years, the cyber insurance market has exploded, as insurers have developed competing products and increased their capacity to meet burgeoning demand from a variety of sectors for protection from risks relating to electronic data losses or security breaches. More than 30 carriers now offer at least one cyber insurance product.[12] These products generally provide liability coverage for privacy-breach claims; many offer other coverage options

---

[4] *See* RT, "SkyJack: Hacker-Drone That Can Wirelessly Hijack & Control Other Drones," https://www.rt.com/news/hacker-drone-aircraft-parrot-704/ (Dec. 6, 2013).

[5] *See* K. Moskvitch, "Are Drones the Next Target for Hackers?," *BBC*, http://www.bbc.com/future/story/20140206-can-drones-be-hacked?ocid=ww.social.link.email (Feb. 6, 2014).

[6] *See* Kashmir Hill, "Here's What It Looks Like When a 'Smart Toilet' Gets Hacked," *Forbes*, http://www.forbes.com/sites/kashmirhill/2013/08/15/heres-what-it-looks-like-when-a-smart-toilet-gets-hacked-video/ (Aug. 15, 2013).

[7] *See* Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway — With Me in It," *Wired*, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (July 21, 2015).

[8] *See* Tarun Wadhwa, "Yes, You Can Hack a Pacemaker (and Other Medical Devices Too)," *Forbes*, http://www.forbes.com/sites/singularity/2012/12/06/yes-you-can-hack-a-pacemaker-and-other-medical-devices-too/ (Dec. 6, 2012).

[9] Lloyd's Emerging Risk Report, *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid* (May 2015), *available at* http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

[10] *Id*. at 11-13.

[11] *Id*. at 16-19.

[12] *See* Richard S. Betterley, *The Betterley Report: Cyber/Privacy Insurance Market Survey 2015*, at 18–23 (June 2015).

including coverage for response costs in the event of a data breach, media liability, first-party property (destruction of data), first-party theft of data, and cyber extortion.

The problem with most of the currently available cyber insurance products is this: They expressly *exclude* physical bodily injury and property damage. These are no doubt intended as "dovetailing" exclusions: to prevent the cyber policies from duplicating the coverage traditionally afforded by general liability and first-party property policies. But do those more conventional policies cover bodily injury or property damage when it arises from a cyber-related peril? In this paper, we discuss the nature and scope of bodily injury and property damage risks stemming from data security failures, and analyze the coverage options available to protect against such risks.

I. Cyber Risks of Bodily Injury or Property Damage.

As Lucy Thomson explains in her analysis of *Cyber Physical Risks*,[13] in the past fifteen years, several cyber attacks have caused significant property damage or bodily injury — and it is only a matter of time before more such attacks occur. Hackers have remotely derailed trains, pumped raw sewage onto public and private property, modified HVAC systems in hospitals with vulnerable patients, and disabled oil pipeline leak-detection systems and nuclear power plant safety monitoring systems.[14] In 2014, the German government released a report that hackers manipulated the control systems at a German steel mill that prevented a blast furnace from shutting down properly, resulting in "massive" (but unspecified) damage.[15] And most recently, in December 2015, a hacker group caused a widespread power outage in Ukraine for several hours, potentially causing property damage and cutting off heat for tens of thousands of people.[16]

In addition to headline-grabbing attacks like these on critical infrastructure and industrial control systems, the burgeoning Internet of Things — networked consumer products and devices, from children's toys to kitchen appliances to medical devices, numbering over 50 billion objects by some estimates and growing daily — presents new potential risks for cyber attacks causing physical harm. These risks may be relevant to an ever broadening range of policyholders, including the growing ranks of companies that manufacture or use such products.

II. Liability Insurance Coverage for Bodily Injury or Property Damage Caused by Cyber Attacks.

Although cyber insurance is now widely available, nearly all of the widely available cyber insurance products currently exclude third-party liability coverage for bodily injury and property damage. A common explanation provided for this near-universal exclusion is that

---

[13] Lucy L. Thomson, *Cyber Physical Risks*, ABA Litigation Section Insurance Coverage Litigation Committee (2016).

[14] *See id.* at 7–9.

[15] *See id.* at 12.

[16] *See id.* at 9–10.

"such losses are covered under CGL . . . policies."[17] But in fact, many recent CGL policies now incorporate their own cyber-related exclusions — the scope of which is not always clear.

A. Commercial General Liability Policies

Over the past fifteen years, Coverage A (the bodily injury and property damage liability coverage part) of the standard CGL policy has been revised several times 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.[18] Next, in 2004, the standard CGL policy 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 data." Thus, damage to physical property caused by loss of electronic data was excluded by this "Exclusion P."[19] In 2013, the standard CGL policy added a sentence to Exclusion P that carved out from the exclusion any "liability for damages because of 'bodily injury.'"[20] That is to say, coverage was *preserved* for bodily injury arising out of the loss of electronic data.

In May 2014, the Insurance Services Office (ISO) published two versions of an endorsement that revises Exclusion P: one with a "limited bodily injury exception" and one without. (Excerpts from these endorsements are appended to this paper.[21]) The latter

---

[17] Robert Bregman, "Cyber and Privacy Insurance Coverage," 37 IRMI, *The Risk Report*, no. 11, July 2015, at 1 ("The [cyber] policies exclude claims alleging bodily injury and property damage because such losses are covered under CGL/property insurance policies.").

[18] 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."

Note that property damage is defined as physical injury to tangible property (including resulting loss of use of that property) and loss 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).

[19] *See* ISO Properties, Inc., *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."

[20] *See* Insurance Services Office, Inc., *Commercial General Liability Coverage Form, CG 00 01 04 13* § I.A.2.p, at 5 (2012).

[21] ISO also published a third version that applies only to Coverage B (and thus omitting the revisions to Exclusion P in Coverage A). *See* Insurance Services Office, Inc., *Exclusion —*

endorsement in part reverts to the 2004 variant of Exclusion P — simply excluding any damages arising out of the loss of electronic data, regardless of whether the damages are because of bodily injury or property damage.[22] The former endorsement in part adheres to the 2013 edition of Exclusion P, which carves out of that exclusion damages because of bodily injury.[23] What's new and identical in both endorsements is the addition of what is numbered 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."[24]

1. Paragraph (1): "Access to . . . Nonpublic Information."

On its face, this new exclusion in Paragraph (1) of Exclusion P appears to be aimed solely at data breaches of private information, and would not go so far as to exclude traditional, physical bodily injury and property damage whenever the cause happens to involve an intruder accessing nonpublic data. But the terms "access to" and "nonpublic information" are undefined. In isolation, they are sufficiently unclear that an aggressive insurer might argue, for example,

---

Access or Disclosure of Confidential or Personal Information (Coverage B Only), CG 21 08 05 14 (2013).

[22] 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., *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).

[23] 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 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. . . . However, unless paragraph (1) above applies, this exclusion does not apply to damages because of 'bodily injury'."

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).

[24] *See* notes 22 and 23 above.

that a hospital's or a 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."

In context, the better interpretation of this exclusion is that it does not stretch so far as to 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 types of access to nonpublic electronic data that regulates networked "things." This is so for several reasons:

- *"Nonpublic Information." — First*, the settings and controls of devices and machinery, though not necessarily accessible to the "public," are not reasonably construed as the types of "nonpublic information" contemplated by the exclusion. The interpretive canon of *ejusdem generis*[25] instructs us that when a series of items in a list all share a certain core characteristic, a "catchall" term at the end of the list should not be read to extend unreasonably broadly beyond what the more specifically listed items have in common. In these endorsements, all of the listed types of "nonpublic information" are primary examples of traditionally confidential information whose confidentiality is recognized, and protected, by law.[26] 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 "trade secrets, processing methods, customer lists, financial information, credit card information, [and] health information." Accordingly, the catch-all term "and any other nonpublic information" in the exclusion endorsements should be read to capture other categories of information whose confidentiality is recognized under and protected by the law. It cannot reasonably be construed to sweep so far beyond the other listed terms as to encompass electronic control systems.

This reading is reinforced by the statement in both endorsements that lists 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."

---

[25] "Under the principle of *ejusdem generis*, when a general term follows a specific one, the general term should be understood as a reference to subjects akin to the one with specific enumeration." *Norfolk & W. Ry. Co. v. Am. Train Dispatchers Ass'n*, 499 U.S. 117, 129 (1991).

[26] The exclusion's list of various types of "confidential information" necessarily starts after the first term, "patents." The presence of this term in the exclusion can only be attributed to sloppy or uninformed drafting, because a defining characteristic of patents is that they are publicly disclosed.

All of these types of expense have become 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 passage's focus on privacy-breach damages reinforces the conclusion that the exclusion was intended only for privacy-related liabilities and does not extend to physical harm that happens to have resulted from a malfunctioning electronic device.

- *"Access To." — Second*, although manipulation of a machine or device's settings may involve "access to" those settings, the scenarios we are concerned with 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 programming bug). In context, the exclusion for damages "arising out of . . . [a]ny access to or disclosure of . . . nonpublic information" means damages arising out of *obtaining* nonpublic information — the type of damages that typically arise from privacy breaches. When the hacking of industrial control systems or networked devices results in physical harm, by contrast, the originating cause is not the *obtaining* of nonpublic information, *i.e.*, 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. The types of hacking that affect the operations of networked devices do not arise out of accessing any *data* relating to those devices, which is what the exclusion requires. It is immaterial that the physical harms in these scenarios arise out of someone's access to the *system or location* where the "nonpublic 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 the substantive content of that original information is essentially beside the point: the harm arises from the newly introduced malicious information. Therefore, the physical harms do not arise from access to the "nonpublic information" itself, and the exclusion does not apply.

- *Extrinsic Evidence. — Third*, reading this exclusion broadly to remove from coverage all sorts of traditional bodily injury and property damage merely because an early link in the causal chain of events involved "access to . . . nonpublic information" would be inconsistent with insurers' contemporaneous explanations of this endorsement. The memorandum that ISO submitted to regulators 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."[27] Although the memorandum also notes that the endorsement

[27] Insurance Services Offices, Inc., *Access or Disclosures of Confidential or Personal Information Exclusions Introduced*, Commercial Lines Forms Filing CL-2013-ODBFR, at 7, 8 (2013), *available at* http://www.serff.com/index_sfa.htm.

without the "limited bodily injury exception" would "result in a reduction of coverage," the memorandum is clear that this statement applies only to the extent that that endorsement reverts from the 2013 amendment of Exclusion P with respect to the loss of electronic data.[28] ISO's express intent not to reduce coverage, and to limit the new exclusion to the types of risks that are covered by common cyber liability policies, is consistent with an ISO executive's explanation at the time the endorsements were introduced, suggesting that the new exclusions were intended to dovetail with coverage available under freestanding cyber policies.[29] Neither the freestanding ISO cyber policies he referenced nor any other commonly available cyber policy form provides coverage for traditional physical bodily injury and property damage caused by rogue electronic devices.

2. Paragraph (2): "Loss of . . . Electronic Data."

The exclusion numbered 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 above, since 2014 this exclusion comes in two different versions. The "limited bodily injury exception" formulation, like the 2013 standard CGL policy, expressly does not apply to damages because of bodily injury. The other version, like the 2004 standard CGL policy, contains no such express carve-out for bodily injury. In both formulations, as with Paragraph (1), the language of this Paragraph (2) exclusion is unclear with respect to coverage for physical harms arising from hackers overwriting or overriding the controls of electronic devices.

Setting aside the lack of an express bodily-injury carve-out in one of the forms (which clearly preserves coverage for bodily injury despite Paragraph (2)), the plain language of the exclusion focuses on the *loss* of data, which does not necessarily occur in a cyber attack — and even where it does occur, any physical harms that are caused by the hacker altering the behavior of a machine or device do not result from lost data, but rather from the hacker's introduction of *new* instructions. However, an aggressive insurer might argue that a hacker overwriting the instructions for a device constitutes "damage to" or "corruption of" data; or that a distributed

---

[28] *See id.* at 8 ("However, when this endorsement is attached, it will result in a reduction of coverage *due to the deletion of an exception* with respect to damages because of bodily injury arising out of loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate data.").

[29] *See* "ISO Comments on CGL Endorsements for Data Breach Liability Exclusions," *Insurance Journal*, July 18, 2014, *available at* http://www.insurancejournal.com/news/east/2014/07/18/332655.htm (quoting Ron Biederman, assistant vice president, Commercial Casualty at ISO as explaining that the endorsements arose because: "As the exposures to data breaches increased over time, standalone policies started to become available in the marketplace to provide certain coverage with respect to data breach and access to or disclosure of confidential or personal information. For instance, ISO Information Security Protection Policy EC 00 10 contains both first and third party coverage through eight separate insuring agreements which address data breach and other cyber-related exposures.").

denial of service attack or other disruption of the transmission of instructions to a device constitutes "inability to access" or "inability to manipulate" data.

Again, like Paragraph (1), Paragraph (2) should be read in context, so that this exclusion does not swallow up coverage for all traditional bodily injury and property damage, merely because a cyber attack is a direct or indirect cause of that injury or damage.

Some cyber attacks that cause physical harm arise out of the hacker's introduction of new data, such as a new script to control the device. Although such an attack may incidentally involve the overwriting of data, the physical harm does not "arise out of" the loss of the original data. Nor can such harm be considered to be caused by "damage to" or "corruption of" data. Following the principle of *noscitur a sociis*,[30] those terms should be interpreted in light of the other terms in the list: "loss of," "loss of use of," "inability to access," and "inability to manipulate." All of these terms focus on the presence or absence of the original data, not on the harmful effects from the introduction of new, malicious data. Accordingly, harm arising out of such new data does not arise out of "damage to" or "corruption of" the old data within the meaning of this exclusion.

Other cyber attacks, however, may not depend upon the introduction of new data, but rather may involve destruction or disruption of network transmissions or device instructions. Paragraph (2) is ambiguous as to whether physical harms resulting from these types of attacks are excluded from coverage. Ultimately, the question of coverage for such attacks may be fact-intensive and depend upon a careful analysis of how the harm arose: *i.e.*, whether or not the significant cause was the "loss of" data or an "inability" to access or manipulate data.

B. Other Coverage Solutions

Given the foregoing ambiguities with respect to CGL coverage and the growing potential for exposure, many policyholders may want to purchase clearer coverage for risks of physical harm from cyber attacks. One option is a difference-in-conditions cyber insurance policy that drops down and pays losses caused by a security failure that are not covered by an underlying policy due to a cyber exclusion. AIG's CyberEdge PC is one of the few products of which we are aware that currently offers such coverage. However, other coverage options may soon be available in the rapidly evolving insurance market for cyber-related risks.

III. First-Party Property

With respect to first-party property policies, common exclusions may create significant gaps in coverage for certain physical harms resulting from cyber attacks. In particular, the Lloyd's Underwriters Non-Marine Association (NMA) forms NMA 2914 and 2915 exclude from coverage "loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER

[30] "[W]e rely on the principle of *noscitur a sociis* — a word is known by the company it keeps — to 'avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words . . . .'" *Yates v. United States*, 135 S. Ct. 1074, 1085 (2015) (quoting *Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995)).

VIRUS) or loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom." They define the term "COMPUTER VIRUS" as "a set of corrupting, harmful or otherwise unauthorised instructions or code including a set of maliciously introduced unauthorised instructions or code, programmatic or otherwise, that propagate themselves through a computer system or network of whatsoever nature." (The NMA forms except damage directly caused by fire or explosion from these electronic data exclusions.)

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."[31] The ambiguity of the phrase "by electronic means" is only heightened by the form's "carve-out" for losses "arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile." (Arguably, that carve-out might suggest that even damage from a car bomb would be excluded from coverage if the car had electric steering — clearly an unreasonable interpretation.)

Although such standard-form exclusions may create coverage gaps for physical harms from hacked systems, they may not appear in the manuscripted policies or insurer proprietary forms typically sold to large corporate policyholders — or they may be negotiable. The emerging risk of physical property damage arising from hacking of networked devices discussed in this paper is yet another reason why insurance buyers — and their brokers — need to scrutinize property policy forms thoughtfully.

* * *

In sum, both insurers and insureds are confronting a relatively novel set of risks: old-fashioned physical harms arising from newfangled cyber perils. Insureds confronted with these cyber-physical losses will undoubtedly argue that they should be covered under their conventional all-risk general liability and first-party property policies. Puzzled insurer-side claims handlers may well look for reasons why these novel risks — which their actuaries may never have priced into policy premiums — should fall outside the scope of conventional policy terms.

To address these new issues, insureds 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 if those cybersecurity measures fail, affording a hacker unauthorized access.

[31] Lloyd's Market Association, *Terrorism Insurance Physical Loss or Physical Damage Wording*, LMA 3030 (Sept. 1, 2006), *available at* http://www.lmalloyds.com/LMA/Wordings/lma3030.aspx.

- *Understand how all policy language will respond to those risks*: This means at a minimum closely reading the policy terms under cyber, general liability, property and any other potentially applicable lines of coverage, such as 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 the terms of the coverage grant in one line do not align intelligently with the exclusion in another?

- *If possible, plug the gaps and clarify the coverage grants*: Some buyers of insurance may be able to negotiate changes in their existing lines of coverage that clarify coverage specifically for cyber-physical risks. Others may need to explore the purchase of new specialty coverage solutions, such as difference-in-conditions excess coverage.

- *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 may reduce the chances that cyber-physical losses will result in the next wave of coverage litigation.

APPENDIX:
EXCERPTS FROM ISO DATA-RELATED LIABILITY ENDORSEMENTS

Exclusion — Access or Disclosure of Confidential or Personal Information and Data-Related Liability — With Limited Bodily Injury Exception

Commercial General Liability CG 21 06 05 14

A. Exclusion **2.p.** of **Section I — Coverage A — Bodily Injury And Property Damage Liability** is replaced by the following:

2. Exclusions

This insurance does not apply to:

p. Access Or Disclosure Of Confidential Or Personal Information And Data-related Liability

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.

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.

However, unless Paragraph **(1)** above applies, this exclusion does not apply to damages because of "bodily injury".

As used in this exclusion, 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.

Exclusion — Access or Disclosure of Confidential or Personal Information and Data-Related Liability — Limited Bodily Injury Exception Not Included

Commercial General Liability CG 21 07 05 14

A. Exclusion **2.p.** of **Section I — Coverage A — Bodily Injury And Property Damage Liability** is replaced by the following:

2. Exclusions

This insurance does not apply to:

p. Access Or Disclosure Of Confidential Or Personal Information And Data-related Liability

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.

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.

As used in this exclusion, 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.