THE INTERNET OF THINGS: IS YOUR CYBER INSURANCE PROTECTING YOU?

Date: 30 November 2016

Insurance Coverage Alert

By: James E. Scheuermann

When the U.S. Department of Homeland Security, the National Highway Traffic Safety Administration, and the Food and Drug Administration each have issued guidance on the risks to health, safety, and productivity associated with unsecured devices on the so-called Internet of Things ("IoT"), we can reasonably assume that these risks are substantial and of meaningful duration. By one estimate, approximately 23 billion "things" are now part of the IoT.[1] That number may climb to 50 billion things by 2020.[2] Global spending on IoT devices and services was $656 billion in 2014. It is estimated to rise to a whopping $1.7 trillion in 2020.[3] The IoT is not a fad. It is our future. Here, as in most other areas in life, benefits are joined at the hip with risks.

In lay terms, the "IoT" refers to devices that are able to process information through software and computer servers to autonomously connect with and to monitor and control the operations of other devices.[4] The devices currently in the IoT include a host of consumer and healthcare products — window shades, light switches, speed governors on vehicles, CCTV cameras, fitness trackers, pacemakers — and industrial control systems that monitor and operate industrial processes in manufacturing plants, electric generating power plants, and the electrical grid.

The benefits of the IoT will be enormous. These will include greater efficiency, increased productivity, and less waste in the creation and use of products and services, and in the creation of products, services, and capabilities that were the stuff of science fiction just a few decades ago: remotely monitoring and controlling an industrial motor to increase energy efficiency and reduce maintenance, turning on your home lights from your desk at work, remotely monitoring patients with chronic diseases so that visits to the doctor's office are reduced, and countless other capabilities.

The benefits of the IoT, however, come with cyber risks. In October of this year, a cyber attack launched through hundreds of thousands of routine, internet-connected devices such as CCTV cameras, digital video recorders, printers, and routers shut down several large consumer websites.[5] It may be just a matter of time before cyber attacks mounted through the IoT shut down or wreak havoc on industrial manufacturing processes, power plants, the electrical grid, medical devices (e.g., pacemakers, dialysis machines), and consumer products. Industry insiders predict that with millions of unsecured devices throughout the world that can be hacked and synchronized to mount future distributed denial of service attacks, the risks are going to get worse before they get better.[6]

The Department of Homeland Security has described the risks as including "malicious actors manipulating the flow of information to and from network-connected devices or tampering with devices themselves, which can lead to the theft of sensitive data and loss of consumer privacy, interruption of business operations, slowdown of internet functionality through large-scale distributed denial-of-service attacks, and potential disruptions to critical infrastructure."[7]

A corporation may be victimized in an IoT-facilitated attack either because its products were a conduit used in the attack or because it is a target of the attack. When a corporation's products have facilitated a cyber attack, it may find itself facing claims asserted by the victims of the attacks. These claims may seek damages for property damage, bodily injury, business interruption or other forms of economic loss, and data theft. When a corporation is a victim of a cyber attack, it may suffer similar losses.

Faced with these substantial and growing exposures, corporate policyholders will look to their insurance coverage for protection. Cyber insurance is all the rage. But how much coverage would a cyber policy provide to a corporate-insured whose IoT products are highjacked and used in a cyber attack or who is an unfortunate victim of an attack the goal of which is the disruption or destruction of the insured's property or cyber capabilities?

Consider, first, liability exposures.[8] Many cyber policies contain exclusions for third-party claims and damages for (a) physical injury to tangible property, (b) bodily injury, and (c) product recalls, including damage to property containing an allegedly defective product. These sorts of liability exposures, however, may be precisely the types of losses caused by a cyber attack made through the IoT.

Consider, for example, an attack on a critical piece of infrastructure, such as a dam or electric grid, that is conducted through IoT devices.[9] If the attacker also obtains operational control of the dam or grid, the resulting property damage and personal injuries could be enormous. The potential defendants in the resulting class actions could well include: the owner of the infrastructure, the operator, the manufacturers of the devices through which the attack was made, developers of the control system software, developers of the security software providing firewalls and malware protection, and any other designer of those devices.[10] Multiple defendants translates to expensive litigation. (Expensive investigations by regulators are also likely to follow in many industries.) When these defendant-insureds turn to their cyber policies for defense and indemnity coverage, they may well hear from their insurers that the alleged bodily injury and property damage liabilities are excluded based on coverage-defeating interpretations of policy language not drafted with these issues in mind. The insurer's views on coverage are hardly dispositive, however, and the policyholder may need to initiate a coverage action to obtain coverage.

Even if an insured does not face third-party liability as a result of a cyber attack, it may still find that its own computer systems, related hardware (routers, air conditioning systems), and other tangible property (such as the dam, electric generators, related buildings, or the electric grid) have been damaged or rendered inoperable by a cyber attack. Will the policyholder's cyber coverage respond?

Exclusions for certain losses arising out of bodily injury and property damage (other than electronic data) are also not uncommon in first-party cyber policies. When a corporate-insured's computers and its other tangible property are damaged by a cyber attack, it may find its insurer pointing to these exclusions (with or without reasonable justification) to deny coverage. Similarly, if a healthcare provider has treated or is treating a patient with a network-connected medical device (e.g., a dialysis machine) that is hacked, leading to the death of a patient, the provider's cyber insurer may attempt to rely on such exclusions to deny coverage. Again, obtaining coverage from a recalcitrant insurer may require expensive litigation.

Cyber insurance is an important tool for corporate-insureds to manage and reduce cyber risks to vital corporate assets. Yet even Lloyd's of London has noted the uncertainty and ambiguity in the scope of coverage for cyber attacks.[11] Apparent limitations on cyber coverage often can be addressed by negotiation with the insurer in the placement process or by existing coverage under other lines of insurance (e.g., the policyholder's general liability,

first-party property, and specialty lines coverages), but only if the policyholder or its representatives are attuned to the risks and the nuances in policy language. In addition, some insurers are now marketing cyber policies that more clearly afford coverage for bodily injury and property damage claims and losses. When such coverages are available, the insured will want to carefully consider the adequacy of the limits or sublimits of such coverages relative to its exposure and how the policy's self-insurance features (deductibles, self-insured retentions) may operate in various loss scenarios.

In our increasingly interconnected cyber future, prudent policyholders would do well to understand and assess how each of the policies in their insurance program addresses the growing risks represented by the IoT.

Notes:

[1] P. Fornash, P. Schenck, "Cybersecurity: From Months to Milliseconds," *Computer* at pp. 42–43 (48:1, Jan. 2015).

[2] *Id.*

[3] IDC, "Explosive Internet of Things Spending to Reach $1.7 Trillion in 2020," June 2, 2015, available at www.idc.com.

[4] More formally, the IoT may be defined as "the connection of systems and devices with primarily physical purposes (e.g., sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems." U.S. Dept. of Homeland Security, "Strategic Principles for Securing the Internet of Things," at p. 2, n.1, Nov. 15, 2016, available at www.dhs.gov/securingtheiot ("Strategic Principles").

[5] "After cyber attacks, Internet of Things wrestles with making smart devices safer," *Reuters*, Nov. 8, 2016, accessed at www.reuters.com/article/us-cyber-attacks-manufacturers-idUSKBN133199; "Can we secure the internet of things in time to prevent another cyber-attack?", *The Guardian*, Oct. 25, 2016, accessed https://www.theguardian.com/technology/2016/oct/25/ddos-cyber-attack-dyn-internet-of-things.

[6] *See* "Here's how the 'Internet of Things' is being used for major cyber attacks on corporations," *Business Insider*, Oct. 21, 2016, accessed at www.businessinsider.com/internet-of-things-corporate-cyberattacks-2016-10; Lloyd's, "Business Blackout, The Insurance Implications of a Cyber Attack on the U.S. Power Grid," 2015, available at http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf#search='he ("Lloyd's, Business Blackout").

[7] Strategic Principles at p. 2.

[8] There is no one widely used standard cyber insurance policy form. Accordingly, the following remarks are necessarily general and need to be viewed against the backdrop of your current or prospective cyber coverage.

[9] The cyber attack on a dam in New York State in 2013 reportedly was made through a cellular modem. "Iranian Cyber Attack on New York Dam Shows Future of War," *Time*, Mar. 24, 2016, accessed at www.time.com/4270728/iran-cyber-attack-dam-fbi/.
Note also the cyber attack on a German steel mill in 2014, which prevented the mill's control systems from shutting down a blast furnace. German authorities described the resulting damage as "massive." "How to stop

cyber-attacks on your organization," *The Guardian*, Oct. 14, 2015, available at www.theguardian.com/public-leaders-network.

[10] *See* Lloyd's, Business Blackout, at pp. 29, 31.

[11] Lloyd's, Business Blackout at p. 37.

KEY CONTACTS

JAMES E. SCHEUERMANN
SENIOR OF COUNSEL
PITTSBURGH
+1.412.355.6215
JAMES.SCHEUERMANN@KLGATES.COM

