Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

3 Tips For Manufacturers To Insure The Internet Of Things

By **Jeff Sistrunk**

Law360, Los Angeles (September 2, 2016, 1:38 PM ET) -- A recent lawsuit alleging St. Jude Medical failed to place adequate safeguards on the remote tracking capabilities of its pacemakers highlights the risks faced by companies that make wireless products connected to the so-called internet of things.

Manufacturers of IoT products live with the ever-present specter of hacking, which can result in the theft of sensitive consumer data or potentially cause the devices to malfunction and cause property damage, serious bodily injury or even death. Unfortunately, experts say, no single insurance policy currently on the market will tackle all the potential exposures faced by internet of things companies.

"It is a dangerous time for a lot of policyholders because they are being steered by insurance market forces into gray areas of coverage," said Joshua Gold, a cyberinsurance attorney at Anderson Kill PC.

Indeed, insurers are modifying both "traditional" liability insurance policies and policies specifically tailored to cyber-related risks in response to the constantly evolving digital threat landscape, according to experts.

“Coverage under both cyber and 'traditional' policies for these risks is changing quickly," said Farella Braun & Martel LLP partner Tyler Gerking. "So companies should not only study their policies closely this year, but set up a process that will encourage them to review these issues annually at renewal time.”

Here, experts discuss the dangers manufacturers of internet of things devices face and how they can insure against those risks.

Shield Against Data Breaches

Like other internet-connected devices, IoT products — including everything from medical equipment to computer-equipped cars to Wi-Fi-capable Barbie dolls — are vulnerable to cyberattacks, which can lead to consumer claims that the manufacturers failed to adequately safeguard their information.

In one of the first suits over purported problems with internet of things devices, St. Jude Medical Inc. was slapped with a proposed consumer class action claiming that the remote monitoring capabilities in its pacemakers are not secure. The Aug. 26 complaint was filed one day after the release of areport by investment and medical researchers that found "severe security vulnerabilities" in the cardiac devices.

While St. Jude has strongly disputed that report as false and misleading, the ensuing putative class

complaint indicates the type of potential liabilities that IoT manufacturers can face due to alleged security deficiencies. The suit claims that patients with St. Jude cardiac implants are susceptible to hackers who might tamper with the data collected via remote monitoring, which allows diagnostic information about the devices to be sent via transmitters to doctors.

Experts say that companies manufacturing internet of things products should seek out specialized cyberinsurance policies, which are designed to cover liabilities associated with data breaches that compromise confidential information. The fact that data is stolen directly from a device rather than a computer server should not matter for purposes of coverage, said Barnes & Thornburg LLP partner Scott Godes.

"You would hope as a cyberinsurance buyer that a privacy or network security incident would be covered under your policy, regardless of whether it is based on an internet of things incident or a more traditional infiltration of a network server," Godes said.

However, cyberinsurance is not necessarily a fail-safe for every type of privacy breach. In the absence of an actual theft of data from an IoT device, some cyber policies may not respond, experts say.

"If a breach results in personally identifiable information being stolen, that presumably would be covered under a cyber policy," said K&L Gates LLPpartner Roberta Anderson. "If the information is simply being viewed, though, that may not be within the scope of coverage."

Fortunately, IoT manufacturers may be able to negotiate with cyber carriers to secure the broadest possible coverage for data breaches, according to experts.

"In cyber policies, a privacy event will be defined in a certain way, and personal information will be defined in a certain way," Anderson said. "Policyholders will want those to be as broad as possible."

Protect Against Product Failures

Perhaps the greatest concern among both manufacturers and consumers is the possibility that hackers could interfere with the proper functioning of IoT devices, which could lead to property damage, bodily injury or death.

Indeed, the report forming the basis for the suit against St. Jude alleged that a hypothetical "crash attack" could, among other things, cause the company's pacemakers to pace at an abnormally rapid rate, potentially leading to severe health consequences for patients. And last year, a pair of security researchers successfully hacked into a Jeep Cherokee's software system and paralyzed the car on the highway, prompting Jeep parent company Fiat Chrysler to recall 1.4 million vehicles to fix a software bug.

A majority of cyber policies don't include coverage for bodily injury and property damage claims, so internet of things manufacturers would need to be sure that they acquire comprehensive commercial general liability policies, which generally do cover such claims, according to experts.

"If you're a manufacturer, you have to make sure that your exposure for property damage, bodily injury or death is picked up somewhere," Gold said.

CGL insurers have begun introducing "electronic data" exclusions into their policies en masse, which

could pose problems for IoT manufacturers seeking coverage for bodily injury or property damage tied to a cyberattack. However, Anderson noted that it may be possible to have an insurer insert an exception to the electronic data exclusion for bodily injury claims.

"That is potentially a major issue for manufacturers of IoT devices," Anderson said. "They will want to make sure there is a bodily injury exception to the electronic data exclusion."

Cover the Executives

Allegations that an IoT device is unsafe can have adverse financial consequences for the manufacturer, including a drop in stock price. For example, the day that the report on the purported cybersecurity shortcomings of St. Jude pacemakers was released, the company's shares fell about 5 percent from the previous day, according to financial information website MarketWatch.

Issues with a company's financial performance often lead to litigation against its directors and officers. While neither St. Jude nor any other IoT manufacturers are currently facing any shareholder class actions or derivative suits over alleged data security failures, experts say such litigation is likely down the road, pointing to the explosion in shareholder claims against retailers such as Target and Home Depot in the wake of major cyberattacks.

Executives of IoT manufacturers should be sure that they have robust D&O insurance coverage in place, particularly if they are required under law to actively oversee and implement the company's cybersecurity programs, experts say.

In general, D&O policies are very broad and will cover individual directors and officers for any acts or omissions while performing their official duties, which would likely include any potential liabilities stemming from an incident causing product failures or the theft of consumer information, according to experts.

At the moment, exclusions for cyber-related events are rare in D&O policies. But as the cybersecurity risks for IoT manufacturers and other companies continue to increase, such exclusions may start to crop up more often, so it is key for policyholders to closely scrutinize D&O products on the market.

--Editing by Katherine Rautenberg and Patricia K. Cole.
