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

5 Questions GCs Should Ask On Securing Internet Of Things

By **Rebecca Eisner, Stephen Lilley and Joe Pennell**
October 17, 2017, 12:25 PM EDT


Rebecca Eisner


Stephen Lilley


Joe Pennell

The rapid growth of the internet of things has brought significant new opportunities for businesses across sectors. From consumer products such as smart homes or connected cars to business implementations in supply chains or delivery networks, these connected devices are creating new markets and new efficiencies for global businesses. But the internet of things also raises a wide range of cybersecurity and data privacy questions for general counsel and their legal teams. Here we discuss five questions for general counsel to consider in managing such cybersecurity risks and data privacy challenges posed by the internet of things.

What Is Our Exposure to the IoT?

Manufacturers and distributors of smart devices such as connected toys or medical devices have obvious interest in the cybersecurity and data privacy risks associated with the products they design, build and sell. But the IoT is a concern not only for manufacturers and distributors of connected devices. A company may rely on smart sensors or other connected devices in manufacturing contexts that may be outside the authority (and risk management processes) of the information technology or security groups. Or a company may be exposed to risk from its vendors' use of IoT devices (e.g., a logistics vendor that relies on various smart tracking tools). Whatever a company's exposure to data privacy and cybersecurity risks from the IoT, understanding those risks will be the first step toward mitigating them.

What Are the Applicable Regulatory Expectations?

Regulators increasingly are focused on ensuring cybersecurity and data privacy with respect to the IoT. The Federal Trade Commission, for example, has taken on a leadership role, including by already bringing enforcement actions against companies that it believed were not taking adequate steps to protect cybersecurity and data privacy in connected devices. In addition, sector-specific regulators have issued guidance for managing cybersecurity and data privacy issues within their respective areas of jurisdiction. The National Highway Traffic Safety Administration, for example, has issued cybersecurity best practices for connected vehicles, and the U.S. Food and Drug Administration has issued guidance for both the premarket and post-market

management of medical device cybersecurity. In addition, data privacy regulations such as the EU General Data Protection Regulation may apply to the data collected by such devices. Understanding how these and other regulatory expectations apply to a company's business will be important to managing the cybersecurity and data privacy risks associated with the IoT.

How Are We Managing Cyberrisk to Connected Devices?

Companies use different tools to mitigate cyberrisks posed by the IoT. A manufacturer of connected devices may use threat modeling and penetration testing to identify vulnerabilities and assess risks prior to product launch, for example, or create a vulnerability disclosure program to manage collaboration with third-party researchers after launch. Or it may use contractual provisions to ensure that its suppliers take comparable steps. Likewise, companies may build governance programs to consistently address cybersecurity and data privacy risks associated with the IoT across their enterprises, whether the connected devices are used by those companies directly or by their critical suppliers.

General counsel will benefit from understanding which of these and other tools their companies have used to manage cyberrisk to connected devices — and how effectively they mitigate related legal risks. This understanding can allow the legal department to provide informed counsel to their clients on how to prioritize and approach internal initiatives that may require different levels of time and engagement. Launching a new program or building security requirements into new contracts may be achievable in the near term. In contrast, changing security expectations in long-standing relationships — for example with suppliers who previously have provided components for nonconnected devices — can require sustained effort and careful negotiation. Armed with a clear-eyed (and preferably privileged) understanding of existing risks, the effectiveness of mitigating controls, and how to prioritize future initiatives, legal departments can help their companies develop practical strategies for enhancing the cybersecurity of connected devices within the realities of corporate budgets, the capabilities of their technical teams, and company culture.

How Are We Managing Data From Connected Devices?

The highly valuable and often sensitive data collected by connected devices offers enormous opportunities for businesses. Allowing businesses to monitor functions, spot patterns and trends, more deeply analyze factors relevant to their operations — and much more — this data is likely to become among the most valuable assets of many businesses.

But this data also presents challenges, particularly when combined with the use of big data analytics. Businesses that purchase IoT solutions, smart devices and related products will benefit from carefully considering data ownership and use rights and from clearly allocating those rights through appropriate contractual terms. Likewise, understanding what information is personally identifiable — or can become personally identifiable once combined with other data sets — is likely to be highly important. Businesses should also evaluate whether any transfers of such data will be performed in compliance with the EU GDPR or other relevant regulations. Moreover, businesses should think through other potential consequences, including whether the collection of such data may increase the burden of responding to document demands by regulators or private litigants (or be used to argue that the data made certain outcomes increasingly foreseeable to those businesses).

What Is Our Litigation Risk?

Cybersecurity and data privacy litigation has long presented substantial risks to companies, particularly

in the aftermath of a data breach. This litigation is now spreading to the IoT, with plaintiffs filing suit over alleged deficiencies in a wide range of connected consumer products. This litigation over cybersecurity and data privacy in the IoT is poised to grow substantially over the coming years. It is not yet clear to what extent such litigation will succeed. Threshold inadequacies in the constitutional standing of prospective class plaintiffs may well defeat such litigation, as may infirmities in the claims pled and in the putative class that the plaintiff seeks to represent. The high stakes of such litigation, however, recommend attention to the potential litigation risk associated with an implementation of IoT devices. Gaining an understanding of those risks (preferably in a privileged context to facilitate candid conversation) will be critical to mitigating those risks.

Rebecca Eisner is partner-in-charge of the Chicago office of Mayer Brown LLP. Stephen Lilley is a partner in the firm's Washington, D.C., office. Joe Pennellis a partner in the firm's Chicago office.