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

Addressing IoT Security: Collaboration Is Key

By **Sonja Carlson, Sheppard Mullin and Alan Brill, Kroll**

Law360, New York (December 20, 2016, 11:35 AM EST) --
The holiday season is here, and internet-of-things gadgets are at the top of holiday lists. 170 million American adults plan to purchase consumer electronics gifts — including wearables, such as smartwatches and fitness trackers, and devices for a smart home, such as smart televisions and wireless toasters — according to Consumer Technology Association data. Yet IoT security is a very real issue, and it is here now.


Sonja S. Carlson


Alan Brill

From a business perspective, it is a mistake to think that IoT security is a future problem that can be kicked down the road. Hackers have increasingly employed IoT devices as bots to orchestrate distributed denial of service (DDoS) attacks, like the attack on domain network service (DNS) provider Dyn earlier this fall, or the network outage that hit hundreds of thousands of Deutsche Telekom customers in Germany last month. Companies face real business risks, as well as potential legal risks — employees, vendors or contractors may have already installed equipment that puts an enterprise at tremendous risk. Such installations were not done with malicious intent but rather, for the most part, because device manufacturers and the companies that purchased and installed the devices did not adequately recognize the risks associated with these unsecured devices.

The economics of turning a blind eye to security concerns often appear compelling — in terms of short-term costs that is. For example, by piggybacking on existing network infrastructure, an enterprise can install a security camera network at all of its locations, thereby benefiting from centralized monitoring, without having to build out a new communication network. In another possible scenario, employees may have installed IoT devices — perhaps variable-color lightbulbs that can be controlled through a smartphone — to make their work environment more pleasant. Yet when a company ignores security issues, it increases the chances that hackers will breach its networks to steal sensitive information, or to launch DDoS attacks targeting other companies or government agencies. The potential for economic loss or reputational harm is, for many companies, much more significant than they realize. Fortunately, companies can take steps to help manage IoT hacking and related risks.

A Collaborative Approach

Security threats used to be considered simply technical matters for the information technology

department or, more recently, the chief information officer (CIO) or chief information security officer (CISO). This approach does not work in today's threat environment. Cybersecurity generally, and IoT security specifically, is an enterprise-wide concern. Cybersecurity is one of the key issues that prevents corporate counsel and board members from getting a good night's sleep. Corporate Board Member's 2016 survey of directors identified cyberrisk as one of the top three issues that needs more time and attention from boards and one of the significant challenges facing public companies.

In terms of responsibilities, it is up to the board of directors to set a company's risk appetite — including its cyberrisk appetite — and high-level cybersecurity policies. The GC and other senior management have a crucial role to play in implementing those policies, making day-to-day decisions regarding cybersecurity issues and potential attacks, and keeping people at all levels of the company informed and educated. This latter point is crucial: To effectively address cybersecurity issues, including IoT security, the board and executive management need to be informed and educated about the constantly developing and changing arena of cyber threats — and so do employees (remember the appeal of remote-controlled, variable-colored light bulbs?).

Perhaps unsurprisingly, there appears to be a gap between senior management and boards' self-perceived understanding and their actual depth of knowledge about cyber issues. A 2016 global study commissioned by endpoint security firm Tanium and the Nasdaq evidences a gap between objective and self-reported cyber literacy. The Tanium/Nasdaq study found that 43 percent of all respondents (which included nonexecutive directors, C-level executives and CIOs/CISOs) were unable to interpret a cybersecurity report at the same level as a financial report, but that in terms of self-reporting in the United States, 59 percent of nonexecutive directors, 77 percent of C-level executives and 78 percent of CIOs/CISOs stated that they were cyber-literate.

The GC is increasingly responsible for cybersecurity matters due to the multifaceted risks that they pose. There are questions of cyber insurance coverage, cost-benefit analyses for cyber-related expenditures, contract terms for global services delivered via the "cloud," and legal risk exposure. The CIO/CISO and IT department best understand the intricate technical aspects of cyber issues and potential solutions, but they, too, need to stay abreast of best practices and developing industry standards. For example, following the October Dyn attack, the National Institute of Standards and Technology (NIST) pushed up the release date to Nov. 15 for its Special Publication 800-160, which detailed best practices for developing secure systems and embedding security into IoT devices, as well as broader goals for starting "a national dialogue" on IoT device security and use. The U.S. Department of Homeland Security issued its "Strategic Principles for Securing the Internet of Things" on the same day. Staying abreast of best practices is important, and enterprises should consider steps to keep executive management current on developments. The CIO/CISO and IT department need to understand — and to be able to effectively communicate — the importance of new technologies and security mechanisms, and help ensure enterprise-wide implementation at all levels and across departments.

Working together in cross-functional collaboration means regular and recurring team communications, and an overarching plan for putting best practices (such as securing IoT devices) into action and timely addressing potential security breaches. The chief financial officer must work closely with the CIO/CISO and GC to understand the technical, business and legal risks in order to make educated and effective budgetary decisions and recommendations to the board. Sufficient financial and human resources need to be allocated to cybersecurity efforts, and the long-term benefits to risk management and the bottom line need to be effectively illustrated. Underlying any effective cybersecurity plan is a basic precept: hackers covet access and information. That means employee information, customer information and financial information. For this reason, the chief human resources officer, the chief marketing officer and

the CFO, respectively, each have important roles to play in helping ensure the security of IoT devices and enterprise networks.

Developing a Plan

There are specific measures that enterprises can undertake now. A collaborative effort that brings together technical, legal, risk-management and corporate-management resources must form the basis of any enterprise-wide plan. To be effective, such a plan should have the backing of the entire organization: horizontal (i.e., cross-functional) and vertical (i.e., board, management and employees). Companies may wish to consider the following action items with regard to IoT security.

First, consider developing a policy regarding what can and cannot be attached to company networks without advance permission. Many companies provide a wireless "visitor's" network that has absolutely no connectivity to networks used for corporate purposes. A company may employ varying rules for such networks, some more effective than others. With a bit of education, employees can make better decisions as to what they attach to even a visitor's network. For corporate networks, more stringent rules should define what devices may be attached and how permission is granted to attach such devices.

Second, combine enhanced network policies with end-user education. If people understand risks and how best to handle those risks, they are far more likely to understand and act in line with policies than if they are not educated on the issue. Incidentally, such educational programs can also help employees avoid cybersecurity problems at home, where IoT connected devices can also cause problems. If a company has a remote workforce, a home network's vulnerability can become the company's vulnerability. Hence, good IoT hygiene at home can be important for both the company and the employee.

Third, given that at-risk devices may already be on an enterprise's networks, have IT run a complete inventory of every device on the enterprise's network. The unique device addresses (called MAC addresses) can usually be used to determine the type of at-risk devices that are on the network. Armed with this understanding, a company can then make decisions as to whether certain attached devices pose too great a risk, and then have those devices disconnected as appropriate.

Fourth, after taking a device inventory, update the network security system settings to either alert IT and the CIO/CISO, as appropriate, when a new device has been attached, or to prevent new devices from successfully joining the network until such devices have been preapproved and their respective MAC addresses loaded into an "approved device" list.

This Issue Isn't Going Away

IoT security and hacking are global problems. Reorienting the way companies approach these issues is key to effective risk management and resiliency in a constantly morphing threat environment. When it comes to IoT security and, more broadly, network security, outside resources are available to help navigate the developing cyber landscape. While some enterprises may have the requisite capability to perform network scans and set up methods for recognizing new threats — e.g., either unexpected hardware or unexpected executable code trying to run on company systems — others may need assistance. Industry standards and best practices, such as those published by NIST, provide some guidance. Consulting and law firms can also provide tailored assistance in establishing a program (which could include policy development, training, tabletop exercises, or network scanning or ongoing monitoring) to get an IoT security program in place that is in line with industry standards.

Sonja S. Carlson is an associate at Sheppard Mullin Richter & Hampton LLP in Washington, D.C., in the corporate practice group.

Alan Brill is senior managing director at Kroll and founder of Kroll's cyber security practice. He consults with companies worldwide on issues relating to the protection of intellectual property in a rapidly changing — and often dangerous — cyber technology environment. Brill often serves as an expert witness or adviser to senior management and boards and he teaches in the Terrorist Use of Cyberspace training program at NATO's Center of Excellence for Defense Against Terrorism.