NIST Guide A Security Blueprint For Connected-Device Makers

By Allison Grande

Law360, New York (November 17, 2016, 10:09 PM EST) -- The National Institute of Standards and Technology has offered connected-device makers fresh guidance on fortifying the growing "internet of things," advising companies to implement security safeguards from the get-go and constantly monitor those systems, an approach that could curtail crippling cyberattacks while helping manufacturers dodge regulatory and legal backlash.

Special Publication 800-160, which was published by NIST on Tuesday and spans 257 pages, presses those involved with developing internet-connected systems and devices to build security safeguards directly into their products and then consider security at every stage in their lifecycle.

"At its core, companies should be encouraged to build in security from the start, just like the NIST guidance proposes," Pillsbury Winthrop Shaw Pittman LLP privacy practice co-chair Brian Finch said. "The internet of things marketplace is still in its early stages, and so there is a unique opportunity here to shape its growth in a way that places security on an equal footing with reliability and functionality. Documents like the NIST guidance can help with doing so."

In its guidance, NIST lays out dozens of technical standards and security principles that developers should be taking into account during every phase of a system or product's lifespan. By pushing manufacturers to consider security at every step rather than worry about threats as they crop up, the agency is effectively offering businesses a way to severely reduce security vulnerabilities that could spell trouble down the road, experts say.

"NIST ... effectively says that security should be built-in by design and reinforced at every decision point along the way," said Katherine Gronberg, the vice president for government affairs at IoT security company ForeScout Technologies. "If universally implemented, it could reduce the number of vulnerable devices deployed worldwide, potentially, by hundreds of thousands or even millions."

Tackling these threats has taken on an added urgency in recent weeks, in the wake of hackers hijacking millions of internet-connected devices to help them carry out a major cyberattack on domain name service provider Dyn last month that temporarily blocked access to popular websites such as Twitter and the New York Times.

"This recent attack was a wake-up call, especially since the group that claimed responsibility for it has said that it was just a dry run for a much larger attack," Duane Morris LLP partner Sandra Jeskie said. "So having guidance that creates a more formalized approach to security and encourages manufacturers to design security into

their devices is an important step to addressing these issues."

The Dyn attack, which prompted NIST to release its new guidance a month early, also raised significant concerns about the potential legal and regulatory liability risks that could arise from security holes that are left unaddressed or are exploited.

"Organizations face known threats but more importantly they face unknown threats and adversary-based threats that are invisible to the organization," said Troutman Sanders LLP partner Steven Gravely. "This creates a significant vulnerability, especially for critical infrastructure industries like healthcare, banking and public utilities."

While the guidance floated by NIST is strictly voluntary, it has the potential to both add to and help cure these liability pitfalls, according to attorneys.

On the one hand, the guidance could present a compliance risk in that "others may come to view it as a best practice, or contractually require its adoption," Jones Day of counsel Jay Johnson said.

Regulators or private litigants looking to take action after an IoT device is compromised could also point to the guidance in an attempt to pin liability on these manufacturers for a breach, as has already happened with the voluntary cybersecurity framework for critical infrastructure that NIST developed in conjunction with the industry and released in 2014.

"The Federal Trade Commission's cybersecurity enforcement actions to date have targeted companies whose security controls were not consistent with the NIST framework, and I would expect a similar approach to the new IoT guidance," Sheppard Mullin Richter & Hampton LLP privacy and security practice co-chair Laura Jehl said. "If regulators and private litigants pursue claims against device manufacturers after a cyber incident, they will almost certainly point to a failure to comply with the NIST guidance as evidence of negligence or lax security."

However, manufacturers can also use the framework to their advantage by taking the time to review the agency's recommendations and making an effort to proactively bake security into their design and development efforts, according to attorneys.

"Part of being cyber-resilient and being defensible to regulators and customers and other stakeholders is to consider what NIST is offering when it comes out with guidance on a critical matter such as increasing security," K&L Gates LLP partner Roberta Anderson said. "So if companies aren't at least considering the standards that NIST has articulated in this guidance, they are doing themselves a disservice."

Chief information security officers and others in charge of cybersecurity at their companies can also seize on the guidance to have vital conversations with executives

about resource and budgetary needs, said Steven Roosa, a co-chair of Holland & Knight LLP's data privacy and security team.

"This is definitely a useful guidemap for security professionals that are responsible for development and security outcomes," he said. "They can use it to go to the board or C-suite and say, 'Look, here are the things we need to do, it's been approved by the U.S. government, and here are the costs associated with these steps.' So it gives them a weapon to go internally to get buy-in and the budget they need."

The guidance could also play a major factor in the increasing push to insure corporations against cyber risks, according to Anderson.

"We've seen underwriters in the cyber insurance realm recently begin underwriting to the NIST cybersecurity framework," she said. "It wouldn't be surprising if insurance underwriters began looking to see how well IoT device manufacturers' protocols and standards and engineering-based security stacks up to what NIST is offering in this new guidance."

The impact of the NIST guidance is likely to be felt well into the future, especially given projections the industry is expected to balloon to include 50 billion connected devices by 2020.

"The rapid proliferation of the internet of things, absent an equal increase in strong cybersecurity protections baked in from the ground up, has already led to several high-profile hacks with troubling consequences, so it's imperative that goods and services are engineered with robust cybersecurity protections in place and not as an afterthought," said Bradley S. Shear, managing partner of Shear Law LLC.

While the FTC, U.S. Department of Homeland Security and other regulators have offered advice on how to protect internet-connected devices and the sensitive data they hold, these guides have homed in more on basic programmatic expectations such as who should be responsible for making security decisions and how to communicate with users about how their data is used.

The NIST guidance, on the other hand, is the first to provide a framework that manufacturers can use to build security directly into their devices.

"Thus, for example, while previous guidance from other agencies and the recently published NIST guidance both focus on the need for 'security by design' and supply-chain diligence, the new NIST guidance provides a first set of engineering principles to achieve these goals," Covington & Burling LLP of counsel Jennifer Martin said.

However, although attorneys widely hailed the NIST approach as a very helpful and promising way forward, they noted that the guidance still presents some pitfalls.

First, convincing manufacturers, especially startups whose primarily objective is to be quick to the market, to invest the time and resources necessary to go through the NIST security exercise could be tricky.

"This is useful and reasonable for 'bigger' companies, but presents challenges and upfront costs for a lot of startups, who don't tend to put time and energy into these issues at the start," Wiley Rein LLP privacy practice chair Kirk Nahra said. "This guidance is telling them that they should — which is of course true — but as guidance may not actually achieve that result."

Jehl added that because many IoT device makers "compete on price," the drive to build cheap, mass-market products that don't contain security features that may impede user experience may override other considerations.

"[Manufacturers] have few incentives to include more expensive security features into their devices unless those features are demanded by their customers," she said. "Any serious effort to secure IoT devices can't rely on technology alone; instead, it will be heavily dependent on educating purchasers about the value of more securely engineered IoT products and persuading them to properly secure them once they're installed."

Convincing companies outside the U.S., where many IoT devices end up being produced, to adhere to security-by-design standards such as the ones advocated by NIST could also throw up a roadblock to the framework achieving its full potential, especially considering that it only takes one weak link in the IoT chain to have a catastrophic effect, attorneys say.

"For the new guidance to make much headway, it will need to be recognized as the standard for IoT security worldwide," Jehl said. "The recent ... attack on Dyn, while felt mostly in the U.S., leveraged millions of unsecured — and likely unsecurable — devices already in use around the world. This is an international problem that will require a concerted effort by manufacturers worldwide."

--Editing by Philip Shea and Catherine Sum.