February 21, 2019

California First to Require IoT Security

CYBERSECURITY, SCHNEIDER DOWNS

BY SCHNEIDER DOWNS PROFESSIONAL

The majority of cyber-attacks are not targeted, rather they are opportunistic, using automated phishing and vulnerability scans. Attackers usually identify the “low-hanging fruit” and investigate further. That’s not to say that attacks cannot be targeted, because when they are, a highly skilled and determined attacker often gets their way.

“Internet of Things” (IoT) devices fall right into the low-hanging fruit category, unfortunately. Due to the generally weak security features of IoT devices, attackers can easily exploit vulnerabilities to spy on or expose your private life.

An IoT device can be any type of physical device with the ability to obtain an IP address and connect to the Internet. By 2020, the population of IoT devices is forecasted to grow to almost 31 billion worldwide, further increasing the probability of compromise. These devices referred to as “smart devices” open the door for attackers to exploit just as any other computing device (i.e., server, desktop/laptop, cell phone, etc.). What if a malicious attacker gained access to your home’s thermostat, security system or video baby monitor? These are the questions that state lawmakers in California are looking to address by introducing Senate Bill No. 327. This bill is the first of its kind that will regulate the cybersecurity of IoT devices.

California Senate Bill No. 327 states that, “*beginning on January 1, 2020 in the state of California, any manufacturer of devices that directly or indirectly connect to the Internet are required to equip the device with ‘reasonable’ security features*.”

What are “reasonable” security features? The bill leaves this to be interpreted. However, the bill requires that these security features be:

- *Appropriate to the nature and function of the device.*
- *Appropriate to the information it may collect, contain and transmit.*
- *Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.*

Also:

- *The preprogrammed password is unique to each device manufactured.*
- *The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.*

While this bill is a good step toward improving the security of IoT devices, it does not address the vulnerabilities associated with IoT devices altogether. Conveyed in a previously published Our Thoughts On article about the Internet of Things, we outline security-focused areas to consider when evaluating IoT devices.

You've heard our thoughts… We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.

Material discussed is meant for informational purposes only, and it is not to be construed as investment, tax, or legal advice. Please note that individual situations can vary. Therefore, this information should be relied upon when coordinated with individual professional advice.