More prevalent than ever before, Internet of Things (“IOT”) devices, a term that includes connected “smart” devices, such as internet connected TVs, wearables, smart speakers, such as the Amazon Echo and Google Home, are fast becoming a staple of how we interact with each other, and obtain and consume entertainment and information. We have previously written about California’s legislation requiring manufacturers to provide reasonable security features “appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, [and] designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.”

The National Institute of Standards and Technology (“NIST”) has recently published two concurrent publications that provide exciting new guidance in this space. IOT device manufacturers have a multipart problem when designing security processes and procedures for their devices. Security will depend on not only the device itself, but also its interactions with human users, and those other resources and systems
that the devices interact with.

**NISTIR 8259** “Foundational Cybersecurity Activities for IoT Device Manufacturers” provides six activities that IOT manufacturers can use to inform primarily the manufacturing of new devices:

1. Identify expected customers and users, and define expected use cases.
2. Research customer cybersecurity needs and goals.
3. Determine how to address customer needs and goals.
4. Plan for adequate support of customer needs and goals.
5. Define approaches for communicating to customers.
6. Decide what to communicate to customers and how to communicate it.

Across these suggested activities, there is a definite emphasis on understanding the customer, including how the customer will interact with the device, how the customer can be informed of security features, and device security lifecycle considerations. Beyond technical measures, such as software, the customer is an integral piece of the proposed security solution – without customer understanding, advanced features and technical countermeasures may not be of much use.

**NISTIR 8259A** “IoT Device Cybersecurity Capability Core Baseline” provides six baseline device cybersecurity capabilities. These baseline elements are meant to be extensible and somewhat solution agnostic in order to provide implementation flexibility. Device manufacturers would do well to review the provided rationales in light of described cybersecurity capability to inform ultimate implementation decisions. The six provided device cybersecurity capabilities are:

1. Device Identification
2. Device Configuration
3. Device Protection
4. Logical Access to Interfaces
5. Software Update
6. Cybersecurity State Awareness

While there is no current requirement that device manufactures explicitly adopt the guidance provided by NIST in these publications, there is a strong likelihood that government authorities will look favorably upon device manufactures that do, including in situations where applicable legislation, such as the California legislation discussed above, do not provide explicit mechanisms or standards to provide required security. If you have any questions relating to how this guidance could be useful for your cybersecurity program, please contact the team at Mintz.
Source URL: https://www.natlawreview.com/article/nist-provides-important-guidance-iot-industry