Historians believe we have started a fourth industrial revolution where physical, digital and biological worlds will merge to form the basis of a new economy. One of the key elements of this transformation is the emergence of the Internet of Things (IoT). Yet the IoT may create havoc if it cannot be adequately secured.

According to Security Today 2018 saw 7 billion IoT devices in use, and there will be more than 75 billion IoT connected devices by 2025. Every second 127 new IoT devices are connected to the web, making it a $1.29 trillion worldwide industry this year. IoT devices are vital to healthcare, autonomous driving, city planning, and consumer’s homes.

But the security issues are exploding too. Although the GDPR and other national laws require security by design, manufacturers are not necessarily building secure devices. Connected device security is expensive and complicated, and when a company is pushing for a small space (like heart monitors) and low prices (like consumer electronics), perfecting security is not the most important design aspect when rushing a product to market.

IoT security weakness often include lack of encryption, insecure interfaces, unneeded network services installed on the device, lack of secure update...
mechanisms, use of outdated components, poor device management, insecure
default settings and lack of physical hardening. Entire connectivity and ecosystem
interfaces may lack adequate security. Data transfer and storage is problematic for
all devices, but particularly where these topics are a low priority in design and
manufacture. Each of these is probably complicated and impactful enough for its own
blog post.

The issue has caught attention in the U.S. Congress. Earlier this month the House of
Representatives unanimously passed the bipartisan Internet of Things (IoT)
Cybersecurity Improvement Act of 2020 to address supply chain risk in the federal
government. The bill would require private organizations selling internet connected
devices to the federal government to notify agencies of known vulnerabilities that
could be used by hackers. Bill sponsor Will Hurd (R-TX) said, “Securing the Internet
of Things is a key vulnerability Congress must address. While IoT devices improve
and enhance nearly every aspect of our society, economy and everyday lives, these
devices must be secure in order to protect Americans’ personal data.” This is the
third IoT security bill to be considered in Congress in the past 4 years.

The bill requires NIST and OMB to update IoT security standards, guidelines and
policies at least every five years. It requires IoT device contractors to adopt
coordinated vulnerability disclosure policies to quickly disseminate known device
vulnerabilities. It prohibits federal agency procurement or use of IoT devices not
complying with the NIST security requirements, with some waivers allowed for
research and other special cases, and it requires NIST to develop reporting
guidelines for security vulnerabilities.

While this bill only applies to federal supply chain purchases, it follows on the heels
of the 2018 California cybersecurity law requiring IoT device manufactures to
implement reasonable security measures appropriate to the nature and function of
the device and appropriate to the types of information it may collect, contain or
transmit, protecting the devise from unauthorized access, destruction, use,
modification or disclosure. The California IoT law is probably best known for calling
out the use of installing default passwords as an unreasonable security practice.

As IoT devices include and operate more important functions in our society, from
personal insulin flow to entire power grids, security becomes more important. Of
course we don’t want hundreds or thousands of the IoT devices to become part of
botnets for denial of service attacks of other mischief, but much of public concern is
directed to the kidnapping of devices to ruin the integrity of their reporting or to
report to a different set of people.

Simple firewalls are not the answer. As noted in a recent ZDNet article, “A perimeter
firewall hasn’t made sense as the way to protect devices since modems and then
smartphones made working outside the office common, just as walled castles are a
bit out of date. Remote connection policies are an attempt to force everyone to go
over the drawbridge where you can take a look at them and their identity papers.
Conditional access policies are like putting someone very experienced on the gate:
even if the identify papers are stolen or a good forgery, they look for suspicious
behavior like having got here impossibly fast or never having been here before but
asking to go straight to the room in the tower with the treasure in.” And this doesn’t
even address lateral passage between rooms in the IoT device castle. Sophisticated
security practice is needed.

A specific illustration of possible harm at a micro level is offered by Dan Goodin in Ars Technica. Dan tells the story of security researcher Martin Hron, who noticed his new $250 “Smarter” coffee maker acted as a Wi-Fi access point using an unsecured connection to communicate with a smartphone app. While this app could allow the user to start making coffee from anywhere, it also allowed unauthenticated access to the coffeemaker’s mechanism that received firmware updates, also with no encryption or code signing. After a week of effort, Hron “could trigger the coffee maker to turn on the burner, dispense water, spin the bean grinder, and display a ransom message, all while beeping repeatedly. Oh, and by the way, the only way to stop the chaos was to unplug the power cord.” The article provides extensive technical details on the hack.

Building effective security into billions of small, inexpensive, often single-purpose devices will be challenging, but we much meet the test. Otherwise an important basis for the new economy will be threatened. More legislators must attend to this issue and force the IoT manufacturers to meet their obligations to us all.

Copyright © 2021 Womble Bond Dickinson (US) LLP All Rights Reserved.

National Law Review, Volume X, Number 275

Source URL: https://www.natlawreview.com/article/will-iot-revolution-be-secured