BOSTON
BUSINESS JOURNAL

Commentary: New U.S. cyber trust mark labeling program is welcome news

BY PETER WINSTON

The Biden administration recently launched its U.S. Cyber Trust Mark cybersecurity labeling program, intended to protect Americans against security risks associated with use of internet-connected devices. As everything the federal government does is in some way controversial, hearing about the plans for a cyber trust mark was a breath of fresh air.

Cyberattacks from "black hat" hackers and bots trying to steal and extort money have escalated. So, too, have cyber-derived terror attacks, such as state and non-state actors working to disable critical infrastructure. With growing hacker access to technology for developing malware and scripting (I'm looking at you, ChatGPT, and your AI-powered friends), these breaches come as little surprise.

Last year alone, more than 422 million individuals were affected by data compromises, including data breaches, leakage and exposure. And there were more than 112 million Internet of Things (IoT) cyberattacks worldwide. That's why I welcome this new program labeling with open arms. It seems like a simple plan to solve an obvious problem from which we can all benefit.

As the CEO of a software development company that creates IoT and embedded devices, I live on the forefront of this world of cyber risk. We're obsessed with cybersecurity. We have to be, for our customers and ourselves. Like most companies today, we've been the target of attacks. So far, we've avoided damage. We depend on an IT strategy based in paranoia and a business strategy that calls for maintaining as little data as possible within our own network.
Our approach is to bake in security from the outset, as I believe it's the most effective way to build well-protected devices. But not all companies or industries use the same approach to device development. Many approach security like a screen door with a flimsy lock that's easy to pick. They rely too heavily on a firewall to safeguard their device, assuming no one cares enough to attack a smart lightbulb or a laser printer. But they're wrong. These seemingly innocuous devices appeal to an entire cast of bad actors.

Peter Winston is founder and CEO of Integrated Computer Solutions (ICS).

Fortunately, U.S. law enforcement is actively in the game, stealthily doing its job to thwart hackers before they strike. But this is a cat-and-mouse game, and the cat is also crafty. In one case at a Las Vegas casino, clever hackers swiped 10 gigabytes of sensitive data by accessing the casino's supposedly protected network through a smart fish tank. The internet connection was intended to enable casino workers to remotely monitor the tank, automate feedings and adjust the temperature. Instead, it provided entrée for some enterprising virtual thieves.

For its part, the FDA has taken action to better protect medical devices as breaches could be life threatening, not just inconvenient. In March they implemented new cybersecurity requirements – stricter rules that device makers must follow – akin to using a steel door with two locks, a deadbolt and a security camera to secure a device.

I applaud the administration's new cyber trust mark labeling program because it will raise the bar for everyone. It's not a mandate – the program is voluntary, modeled after the Energy Star system used for appliances – but the new mark will make it easy for people to identify (and avoid) cheaply made devices plagued with security holes.

Further, the program will allow U.S. cyber command to guide device makers and device users in the right direction without revealing all they know. This is how the government is helping to keep us safe.

Now more than ever, manufacturers need to quickly adapt to keep pace with the evolving threat landscape by addressing cyber shortcomings to better safeguard their products. I believe the new cyber mark program will spur more device manufacturers to do just that.

Peter Winston is founder and CEO of Integrated Computer Solutions (ICS) in Waltham, a custom software developer that creates touchscreen and embedded devices.