Announced within days of one another, two developments, one bureaucratic, one nefarious, showcased the growing chasm between the dream and the reality of our increasingly interconnected world. On December 4, 2020, President Trump signed into law the “Internet of Things Cybersecurity Improvement Act of 2020,” which establishes security standards for Internet of Things (IoT) devices owned or controlled by the Federal government. And this week, with everyone focused on the Electoral College and the Pfizer vaccine, we learned again just how vulnerable the systems we rely upon for, well, just about everything, really are.
As reported in Krebs on Security, Russian hackers (probably) hacked SolarWinds’ Orion platform software that, among other things, helps the federal government and a range of Fortune 500 companies monitor the health of their IT networks. If you have never heard of SolarWinds or its software, the scope of the problem might be lost on you. Make no mistake, it’s kind of a big deal. SolarWinds’ customers include:

- More than 425 of the US Fortune 500
- All ten of the top ten US telecommunications companies
- All five branches of the US Military
- The US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the Office of the President of the United States
- All five of the top five US accounting firms
- Hundreds of universities and colleges worldwide

Here is the eye-opener, as reported by David Sanger and his team at the New York Times: “The National Security Agency — the premier U.S. intelligence organization that both hacks into foreign networks and defends national security agencies from attacks — apparently did not know of the breach in the network-monitoring software made by SolarWinds until it was notified last week by FireEye.” That’s right, the same seemingly all-powerful NSA that just a couple of months ago was in the news when the U.S. Court of Appeals for the Ninth Circuit handed down a ruling that the warrantless telephone dragnet that secretly collected millions of Americans’ telephone records may well have been unconstitutional did not know it had been hacked until FireEye, a private cybersecurity consulting company, told them so. And FireEye itself would not have known either but for its investigation of its own hack.

This brings me to my point: it’s almost 2021 and the US has just now signed into law a bill requiring, among other things, the OMB to “develop and oversee the implementation of policies, principles, standards, or guidelines as necessary to address security vulnerabilities of information systems.” However salutary it is to require more care in how the US government buys connected devices, it sure seems like a belated drop in a very large bucket. In the meantime, everyone from Homeland Security on down is trying to figure out how something as innocuous-looking as a software upgrade could wreak such havoc. It would take someone a lot less jaded than I not to think about horses and barn doors or days late and dollars short.

If you had “Entire Nation Hacked” on your 2020 bingo card, you may collect your winnings on the way out. There is much to be done and in many ways, we are just getting started. To paraphrase the Mishna: The day is short, the work is great, the workers are lazy, the reward is great, and the Russians are pressing.

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

National Law Review, Volume X, Number 352