

Opinion: The Russian hack and securing our 5G broadband future

Matt Walton

Jan. 3, 2021 Updated: Jan. 3, 2021 12:04 p.m.



(FILES) This file photo taken in Barcelona on February 24, 2019 shows Chinese electronics company Xiaomi Corporation's new smartphone Mi MIX3 5G displayed at the Mobile World Congress (MWC), on the eve of the world's biggest mobile fair. - The next allocations of frequencies for 5G should not be done without prior assessment of its impact on the environment, recommends the High Council for the Climate on December 19, 2020, while French President refused to postpone the deployment of this technology. (Photo by LLUIS GENE / AFP) (Photo by LLUIS GENE/AFP via Getty Images)AFP via Getty Images

<https://www.ctpost.com/opinion/article/Opinion-The-Russian-hack-and-securing-our-5G-15842805.php>

Vulnerability

It doesn't look like a four-letter word but, as with all things in the realm of cyberspace and security, looks can be deceiving. News of the Russian hack of literally tens of thousands of government agencies and many of our largest companies has suddenly made our vulnerability painfully real — especially at a time when the pandemic has expanded our use of cyber space into virtually every aspect of daily living. “Work From Home” (WFH), food delivery, on-line retail, telehealth, and distance learning are only examples of a myriad of daily life functions that have suddenly been transformed from in-person to an increasingly digitally accessed world. While empowering, this digital transformation is also creating new digital vulnerabilities.

The bad guy is in the house

That old horror movie line is suddenly a chilling possibility for vast portions of the United States public and private networks. The “high trade craft” introduction of sleeper malware into a seemingly routine upgrade of Solar Winds Orion software between March and June of 2020 has exposed large sectors of U.S. infrastructure to malicious actors who can not only spy on sensitive and secret information, but also invisibly manipulate the underlying systems that actually run key segments of our society. Left unchecked, the potential mischief and real damage is incalculable, and the really scary thing is that, unless we're very careful, they'll be watching us do whatever we try to do to fix it from *inside the house*.

Cyber security is national security

The primary function of our National Security agencies is to protect the American way of life. Increasingly the traditional “analog” threats that have challenged our armed forces and intelligence agencies have been made worse, or supplanted, by cyber threats that have the capacity to inflict both tactical and strategic damage as bad or worse than conventional weapons. The pandemic and the exponential expansion of our use of the Internet has accelerated the pace of our adoption of broadband enabled technologies. The impending widescale deployment of 5G will supercharge the digital transformation. Without the right security systems in place, it will also supercharge our vulnerabilities.

Securing 5G in the broadband ‘landrush’

In the run up to the present, the big telecom providers have rushed to secure as much of the broadband grid as they can get in a chaotic, “land rush” environment. The reality is that this expansion is occurred without effective guidance or oversight from the security agencies, regulatory entities and standards bodies who should be guiding the 5G buildout. Despite the release of “The National Strategy To Secure 5G” in March 2020 (ironically the same month as the Russian hack), the actual implementation of the next generation security protocols and equipment necessary to secure our 5G infrastructure are still aspirational — neither formalized nor reduced to practice.

5G cyber security and power-wiring of America

The primary imperative of private enterprise is to make a profit and increase equity value for shareholders. Though recognized, “security” is generally perceived as a cost of doing business rather than a direct contribution to profit. Consequently, the tendency of most private companies is to default to the minimum — particularly if more comprehensive/effective solutions cost more or delay rollout.

The new administration has announced plans to invest in universal broadband. This national commitment to 5G provides a unique strategic security opportunity to address our national cyber vulnerabilities. In the spirit of “who pays the piper picks the tune,” nationally funded broadband infrastructure investments would give the government (and especially the security agencies) the economic leverage to ensure that the 5G build out incorporates necessary security systems from the start — in the same way the that the build out of the National Highway System in the 1950s and 60s was funded to meet national defense standards.

It is a well-known engineering principle development that the cost of building security in at the beginning is orders of magnitude less expensive than putting it in later. “An ounce of prevention is worth a pound of cure” is the essential element in cyber security.

We have the opportunity to make cyber security a “hardened” part of our national infrastructure as we build out our economy for the post-COVID era. We should take it.

New Haven resident Matt Walton is a partner at McCreightPartners and has served as a senior executive in public, private and non-profit organizations with special focus on information technology, health care, national security, and emergency management. Walton was directly involved in the response to SARS, West Nile Virus, pandemic H1N1 and Ebola.

Written By
Matt Walton