Water, Hospitals and Intellectual Property...the Cyber Risk Surges, Particularly for U.S. Critical Infrastructure

11.04.2022 | By Hon. Chris Carney

In a recent report, Microsoft cataloged the past year's cybersecurity threats they saw plaguing the U.S. What they found is as disturbing as it is unsurprising. China, Russia, Iran and affiliated groups are all becoming far more aggressive in the cyber arena, relentlessly threatening our infrastructure, our healthcare and our intellectual property. For example, the company noted that 54% of all Chinese cyberattacks targeted the United States, with particular emphasis on economic cyber-espionage operations intended to steal intellectual property.

The report also revealed increasingly aggressive and dangerous attacks coming from Russia, with particular concentration on critical infrastructure systems. Ninety percent of all Russian cyberattacks aimed at critical infrastructure were directed at NATO countries, with the U.S. as its primary target. Tom Burt, Microsoft's Vice President of Customer Security and Trust, noted that Russian hackers are particularly keen on going after "organizations in the water sector." We cannot forget the cyberattack on the water treatment facility in Oldsmar, Florida, in the Tampa Bay area in February 2021 that had the potential to sicken or kill thousands of residents.

In addition, the report noted that Iran was becoming far more aggressive in using ransomware attacks against U.S. targets. In mid-September, the Department of Justice (DOJ) indicted three Iranians who launched cyberattacks against key components of our critical infrastructure, including ransomware attacks on healthcare systems, transportation systems and public utilities. And while the DOJ said the attacks were not on behalf of the Tehran government, they were allowed by the Iranian regime.

These state-sponsored and state-affiliated cyberattacks are becoming more persistent and more sophisticated. They are also becoming more costly and potentially more deadly. As these actors prey upon unprepared and under-resourced organizations, our national, economic and environmental security are at risk. An ounce of prevention is much cheaper than the pound of pain cyberattacks will inevitably cause.