HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

ALERT

Issued 8/14/18

While Everyone Obsesses over Russia, China is Stealing our Data Blind

Over the past decade, Chinese hackers have launched cyber-attacks, stealing data from the U.S. Congress, the U.S Department of Defense, and the federal Office of Personnel Management, one of the largest data breaches and thefts of American worker identities in history. The Chinese have run sustained cyber operations against our oil industry, critical infrastructure and utility industries, and the entertainment industry. With trade tensions running higher, China's interest in hacking U.S. private businesses for data, trade secrets and intellectual property has only increased. As noted by Wired magazine, Chinese government-backed hackers are also interested in so-called "command and control" opportunities in the U.S., everything from satellites and main frame computers to in-home laptops and security cameras. Yes, the Chinese are even interested in that nanny cam you may have in your nursery. American consumers, while alarmed by such data breaches as the Yahoo email hack in which almost 3 billion consumers had personally identifiable information stolen, or the various retail chain hacks such as Target and Neiman Marcus, still tend to be lax about the security measures they use and fewer than 15 percent utilize security measures like password keepers to secure access to their important web sites and data like bank and investment accounts, health care information and access to their cloud storage, where they upload everything from legal documents, financial information and tax returns, to family photos, music and movies. The cloud and the access the cloud can enable to home networks is increasingly where consumers should be concerned. Most probably aren't asking where the data from their smart devices is going, or who has access to that data. Nor are they asking what the rules and regulations governing 3rd party access to that data are and where is it actually stored. But they should be. Most consumers are completely unaware that the smart devices, on which they've come to rely for everyday home convenience, transmit data back to a platform that is then stored on "the cloud." When you go to Walmart or Target and buy a camera-enabled smart TV or a baby cam monitor, you don't consider that the digital video feed might be transmitted to and stored in a cloud outside the United States and viewed by a hostile, foreign government like the Chinese. But that is exactly what is happening. Those smart, internet of things (IoT) devices, which numbered just over 8 billion in 2017, require platforms to "plug into" and a significant amount of those devices have agreements with platforms controlled by Chinese nationals with obvious ties to the Chinese government. That's right, not kidding: the communist Chinese government may have access to your home via those smart devices. This entire trend of the internet of things and smart devices is only going to accelerate: there are estimates that by 2020 there will be over 20 billion IoT devices, all plugged in to some platform somewhere. What retailers are not telling you is that those technological wonders likely rely on platforms and cloud storage controlled by Chinese nationals.