Sheldon Jacobson: Russian cyberattacks are a threat. But so is Americans' fear of shortages.

Jacobson, Sheldon . Chicago Tribune (Online) , Chicago: Tribune Publishing Company, LLC. Mar 28, 2022.

FULL TEXT

Reports of Russian cyberattacks against our domestic infrastructure have raised alarms and calls for heightened vigilance across the United States' public and private sectors. Given that the U.S. and its allies have imposed significant economic sanctions against Russia for its attack of Ukraine, state-sponsored Russian cyberattacks are likely; they may be viewed as an effective form of retaliation.

Domestic infrastructure, including our nation's power grid, food supply chain, water systems, financial system and government agencies, have all been targets of cyberattacks for years.

For example, last spring, ransomware attacks against the Colonial pipeline and meat producer JBS temporarily disrupted fuel and food supply chains. The attacks were traced to an organization based in Russia. Its motives were clearly financial —secure payments from large organizations with deep pockets that cannot afford such a disruption to their operations and supply chains.

Are cyberthreats from state-sponsored Russian operatives potentially more lethal? The problem is differentiating between state-sponsored attacks and attacks by cybercriminals. Their motives may be different, but the tools that they use still require penetrating cybersecurity walls through weak links, such as by exploiting vulnerabilities in multifactor authorization protocols.

The recent warning about possible state-sponsored Russian cyberattacks reminds us that every entity, large or small, is vulnerable if it lets its cybersecurity guard down. This has led to significant growth in the cybersecurity industry, as more bad actors attempt to penetrate the cyber infrastructures of companies and organizations. The cybersecurity market is estimated to reach over $366 billion by 2028.

Ironically, the most sophisticated firewalls and cybersecurity guards are only as safe as the people who use them. Cybersecurity often requires that people take extra steps to ensure that their computer systems are protected. If just one person lets their guard down, such as by opening an innocuous-looking email attachment that is actually a form of phishing, a perpetrator will be able to bypass sophisticated protections and gain access to valuable information behind a firewall.

Russian cyberthreats are not new. The statement President Joe Biden issued for heightened vigilance is not only applicable today but also should be part of the daily protocol for every company and organization. Whether it is maintaining state-of-the-art firewalls and identity validation systems or training people to follow the most up-to-date security procedures, protecting every entity's cyber infrastructure must be a top priority.

One major threat of potential Russian cyberattacks is an overreaction by Americans as they fear disruptions in gasoline, food, banking or other commodities and create a surge in demand and artificial short-term supply shortages. Such events would also temporarily drive prices higher, further fueling inflation pressures that are already at a 40-year high. This means that the American people, not the Russian government, would be creating havoc in the U.S. economy.

As war in Ukraine rages on and Ukrainians valiantly fight to protect their homeland, the cyber war in the United States has been happening for decades. The most recent alarms over Russian cyberattacks are just another battle

to be considered in the cyber arena.

Should Americans be concerned about their gasoline, food or energy supplies? No more so than they were last month or last year. The biggest threats come when known vulnerabilities are not immediately resolved and when people let down their cybersecurity guard and allow bad actors in.

Then the worst-case scenario may become our reality.

Sheldon H. Jacobson is a professor of computer science at the University of Illinois at Urbana-Champaign.

Submit a letter, of no more than 400 words, to the editor here or email letters@chicagotribune.com.

DETAILS

Subject:	Food supply; Internet crime; Supply chains; Food; Infrastructure; Computer security
Business indexing term:	Subject: Supply chains Infrastructure
Location:	Russia; United States--US; Ukraine
Publication title:	Chicago Tribune (Online); Chicago
Publication year:	2022
Publication date:	Mar 28, 2022
Section:	Opinion - Commentary
Publisher:	Tribune Publishing Company, LLC
Place of publication:	Chicago
Country of publication:	United States, Chicago
Publication subject:	General Interest Periodicals--United States
Source type:	Blog, Podcast, or Website
Language of publication:	English
Document type:	Opinions
ProQuest document ID:	2644133255
Document URL:	https://www.proquest.com/blogs-podcasts-websites/sheldon-jacobson-russian-cyberattacks-are-threat/docview/2644133255/se-2?accountid=14553
Copyright:	Copyright Tribune Publishing Company, LLC Mar 28, 2022
Last updated:	2022-03-29
Database:	Chicago Tribune

LINKS

Check for FullText Availability