Cybersecurity’s bad and it’s getting worse

washingtonpost.com/politics/2022/06/24/cybersecuritys-bad-its-getting-worse

Joseph Marks, Aaron Schaffer June 24, 2022

Welcome to The Cybersecurity 202! This is my last newsletter after three-and-a-half years as author of The Cybersecurity 202. It’s been a blast!

Thank you!: To editors who guided me; researchers who wrote far more of this newsletter than most people realize and frequently caught my errors before they got into print; fellow reporters at The Post and elsewhere; sources without whom this newsletter would not have been possible, especially those who spent hours patiently explaining complex issues to me (you know who you are); and to readers who always gave me great feedback and made the newsletter better.

As for me: I’ll be heading to Johannesburg, where my wife will be doing her first tour as a U.S. Foreign Service officer. I’ll be doing some freelance reporting, so send any South Africa stories and tips my way. **Please stay in touch**. You’ll still be able to find me on Twitter. Other contact info is in my bio there.

It's hard to overstate how much cybersecurity has surged as a top concern

---

There are few analogues in history for how cybersecurity has surged in importance as a government policy issue during the past eight years.

It's gone from a relatively back-burner issue embraced by a handful of government officials and lawmakers to a top national security concern — one that prompts partisan squabbles in Congress and heated confrontations between U.S. and Russian presidents.

And that's probably just the beginning. Things will definitely get wilder from here.

This is my last Cybersecurity 202 after three-and-a-half years authoring this newsletter and eight years as a journalist on the cyber beat.

Eight years is a long time on any beat. It's several lifetimes on this one.

Here are three big themes that have preoccupied my reporting the past eight years.

Bigger, bigger, BIGGER

Cybersecurity wasn't unimportant when I started on this beat in April 2014. But it was a shadowy topic, more fretted about than understood. When cyber news stories broke through to mainstream audiences, they were usually about credit and debit card breaches that had limited real impact on consumers except the few who suffered identity theft.

The big story at the time was a mammoth credit card breach at Target that had forced the big box retailer's CEO to resign — a cataclysmic event for industry then that's largely a footnote now.

Things changed quickly.

- Within a few months, there began a series of major events that would redefine the role of cyberthreats and cybersecurity in the national conversation.
- The year 2014 alone included the first U.S. indictments against Chinese government-backed hackers and the Pyongyang-backed hack of Sony Pictures Entertainment after North Korean leader Kim Jong Un objected to one of the studio's movies. Within weeks of the Sony attack, during the first days of 2015, the Obama administration imposed the first-ever sanctions for a cyberattack on North Korea.
- Then came the FBI's push to mandate government back doors in encryption systems, Russian hackers' efforts to interfere in the 2016 elections, a series of devastating criminal ransomware attacks against U.S. critical industries, and on and on and on.

With each passing year, cyber insecurity became a more fundamental and important aspect of U.S. policy, politics and daily life — similar to how connected technology itself had become increasingly pervasive a decade or two earlier.

By 2022, the prefix “cyber” has begun to seem anachronistic because digital conflict and crime is more the standard than the outlier.

Criminal ransomware gangs, for example, draw far more attention these days than conventional organized crime. And even the mafia is getting into hacking to support traditional criminal pursuits such as drug trafficking and extortion.

The cyber component of Russia’s Ukraine invasion has been more limited than some experts predicted. But it still underscores that cyber operations are sure to be a component of every future military conflict.

Lots of big talk, little real change

U.S. cyber protections have, by and large, not remotely kept pace with the threat.

The vast majority of companies are still compromised by hackers because of simple and preventable lapses, such as using shoddy passwords, not updating commercial software and employees getting conned by phishing scams that they should be wise to.

Why?

There are a lot of possible explanations, including corporate apathy and a structural advantage held by hackers.

One big explanation, though, is that government and other large institutions haven’t done the necessary work to change companies’ incentives to make cyberattacks less common. That’s unlikely to change soon.

The years-long wave of increasingly brutal and consequential cyberattacks has not been accompanied by big legislative changes.

- It was only this year that Congress mandated that some companies report to the government when they’re hacked. The law only applies to firms in critical industry sectors such as finance, energy and health care, and it may not go into effect until 2024.
- That’s a big improvement but an exceedingly minor requirement considering the roughly $1 trillion that McAfee estimates is lost to cybercrime each year.

Federal agencies have mildly ramped-up cyber requirements in a handful of critical industry sectors, including pipelines and rail transport but to decidedly mixed reviews from the regulated companies.

> White House officials say they’re unable to move harder on regulation without specific authorization from Congress.

Many hoped that cyber insurance policies would force companies to adopt better practices to maintain coverage.

> What's mostly happened instead is that insurers have competed for customers by making compliance less onerous. They've often failed to verify that companies are following the requirements they do put in place.

Which brings us to the third big theme …

Things will get worse before they get better

This is about as easy as predictions get given the course of the past eight years. Everything got worse — often in unexpected ways.

The cyber future is especially treacherous because of a number of powerful new technologies that will integrate the internet ever more deeply into the fabric of daily life — including 5G wireless networks, artificial intelligence and connected technologies such as smart thermostats.

That will give hackers significantly more power to cause damage.

Then there are the unknown threats. Given the pace of technology development, it's likely the nation will be hit within the decade by forms of cyberattacks that are hardly conceivable today.

The topic reminds me of an interview I conducted with a former contractor for the Defense Advanced Research Projects Agency (DARPA) who wrote a report about looming cyberthreats in the year 2000. The report was released publicly for the first time in 2018 as part of a broad public information request by George Washington University's National Security Archive of emails and documents shared with former Defense secretary **Donald Rumsfeld**.

The report presciently noted how early the nation was in cyberwarfare developments — comparing it to the state of air warfare in the years before World War I.

More than 20 years later, those unknowns are even bigger because — largely because the internet touches not just warfare but nearly every facet of modern life from business and commerce to entertainment and romance. It's unlikely we're anywhere near a stable point in cyber development where we can speak with confidence about the future.

But I'm curious to see what happens.