THE HILL

It's time to secure our digital sidewalks

BY JORDAN SUN, OPINION CONTRIBUTOR — 11/25/20 03:00 PM EST

Just In...

Judge directs state officials not to reset Georgia voting machines
STATE WATCH — 3M 18S AGO

The Hill's 12:30 Report - Presented by Capital One - Biden unveils batch of his White House team
12:30 REPORT — 9M AGO

In the wake of the 2020 presidential election, here's how business leaders can make America fairer, faster
CHANGING AMERICA — 12M 32S AGO

GM pulls planned backing from electric vehicle company
ENERGY & ENVIRONMENT — 14M 20S AGO

Is America breaking its health care promise to you?
OPINION — 19M 46S AGO

US sanctions Chinese company for conducting business with Maduro regime
NATIONAL SECURITY — 27M 36S AGO

Rand Paul says Fauci owes parents and students an apology over pandemic measures
NEWS — 47M 57S AGO

Moderate Democrats: Everyone's older siblings
OPINION — 49M 46S AGO

VIEW ALL

View Latest Opinions >>

© iStockphoto

Prior to COVID-19, the U.S. Federal Communications Commission (FCC) estimated at least 30 million Americans were on the wrong side of the digital divide, and nearly 12 million children are part of "the homework gap" because they do not have access to broadband internet at home. Local and state governments across America have moved to fight the digital divide thanks to the leadership of elected and administrative officials, the frontline efforts of not-for-profits, and the support from corporate and private philanthropists. As we collectively move forward to bring millions of Americans online (sometimes for the very first time), we are also exposing our communities to new risks in this "new normal," virtual world.

Cybersecurity experts have projected that cybercrime will cost the global economy as much as $6 trillion across today's 4.57 billion internet users. For 2020, cyber incidents continue to haunt our headlines. During just the last few months in the U.S., we have seen unprecedented cyber incidents — from United Health System's incident that affected 250 facilities to two Westchester school districts reporting data breaches to racist Zoombombing of Connecticut's Congresswoman Jahana Hayes.

All of this in the midst of unprecedented change everywhere we look.

In response to COVID-19, most Americans rushed into the new era of a remote and digital world. We left behind our concrete sidewalks and flooded our *digital sidewalks*. If you imagine a typical city's physical sidewalks, they are usually secured by local businesses, pedestrians, nosy residents, vehicles, and law enforcement. In the real world, would you worry if your elderly parent went out for a stroll at 1 a.m.? If you are a parent, how comfortable are you allowing your underage children to play on the sidewalks unsupervised — during the day or night?

But now, on these crowded *digital sidewalks,* Americans are conducting unprecedented commerce, education and learning, entertainment and media, civic engagement and political action, communication with family and friends, financial transactions, access to government services, and, of course, remote work for those fortunate enough to telecommute during this recession. Nevertheless, this is the new world that we live in, and — to borrow from a common military phrase — we as a people must *improvise, adapt, and overcome* our new virtual environment and its increasing cyber risks.

So, when we invest in crossing the digital divide, why not also talk about how cyber threats can impact our most at-risk populations, especially communities of color, immigrants, elderly, children, and handicapped individuals?

As of 2019, cybercriminals are stealing nearly $40 billion annually from vulnerable older adults. Federal law enforcement have also warned schools that "cyber actors are likely to increase targeting of K-12 schools during the COVID-19 pandemic because they represent an opportunistic target as more of these institutions transition to distance learning." This is on top of the growing incidents of cyberbullying and hate speech due to increased screen time from children.

Some cities have already pursued initiatives to address the issue of online safety and security. Here in San José, under Mayor Sam Liccardo's leadership, our $24 million Digital Inclusion Fund, a public-private partnership with the major telecommunication companies and administered by the California Emerging Technology Fund, emphasizes investing not only in connectivity and devices but more importantly in digital literacy. Back in 2018, New York City's Cyber Command pioneered — in partnership with mobile security company Zimperium — NYC Secure, a free, city-funded iOS and Android app that will alert New Yorkers if their mobile device or tablet encounters threats (i.e. unsecure Wi-Fi networks) and will also recommend how to address the threats without sacrificing user privacy. Digital Charlotte in North Carolina empowers organizations in their community to deliver not only digital literacy training but also to provide media literacy resources.

While programs like this are a good start, state and local governments need to proactively do more to *adapt and overcome* our residents' new public space for convening — the *digital sidewalk* — and the increasing cyber and information operations risks in the "new normal." State and local governments are facing an ever evolving, innovative threat seeking to deceive, degrade, deny, disrupt, and even destroy our communities' abilities to recover. We are in uncharted waters with state and non-state actors' cyber and information operations activities threatening our privacy, livelihoods, personal safety, and democratic institutions.

We need to recognize that while we might not be as fast and nimble as our attackers, we can hold the line by encouraging collaborative learning, best practices, and incidence sharing between local and federal agencies.

Local government Chief Information Security Officers (CISOs) should also consider (and be more empowered with) their unintentionally expanded role in protecting their residents and not just enterprise IT infrastructure.

First and foremost, state and local government leaders need to acknowledge the significance of our cyber challenges and the critical investments needed to *secure our digital sidewalks*. Therefore, I call on government, industry, and community leaders to reimagine, together, how our digital inclusion mission has evolved as we bring millions of Americans across the digital divide at unprecedented speed and scale.

Jordan Sun is the Chief Innovation Officer for the city of San Jose and Director of the Mayor's Office of Technology and Innovation (MOTI). Previously, was deployed to Afghanistan as the Chief Operating Officer for the Special Operations Joint Task Force-Afghanistan Technology Team. He holds the rank of Major as a reservist supporting the Army's technology modernization efforts and was previously with In-Q-Tel's Menlo Park Investments Team. Before deploying, he was the director of venture development at Siemens Healthineers' Digital Incubator, where he led a digital health spinout venture as CEO. He also held commercial leadership roles in medical technology based in the Bay Area and Asia.

TAGS JAHANA HAYES CYBERCRIME COMPUTER SECURITY CYBERATTACK DIGITAL LITERACY DIGITAL DIVIDE SOCIAL INEQUALITY WORK FROM HOME DISTANCE LEARNING ONLINE EDUCATION

THE HILL 1625 K STREET, NW SUITE 900 WASHINGTON DC 20006 | 202-628-8500 TEL | 202-628-8503 FAX