Protecting 'Digital Sidewalks'

Governments are embracing a new cybersecurity strategy as an integral part of their civic responsibility.

COVID-19 has led to a "cyber pandemic"[1] in the public sector, as more sophisticated security threats target government organizations and the constituents they serve.

While state and local governments have focused on strengthening internal security, they must also focus on ensuring constituents' data is secure — especially as they expand public Wi-Fi access points, build out their broadband infrastructure to bolster smart city initiatives and provide constituent-facing, self-service digital applications.

Digital safety is now public safety. Strong cybersecurity has become just as integral to public safety as police, fire and emergency management functions. As Jordan Sun, the chief innovation officer for the city of San José, has put it: It's time for state and local governments to secure their "digital sidewalks."[2]

"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," Sun wrote in an essay in *The Hill*, a Washington, D.C., newspaper. "[O]n 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."

“Ultimately, we wanted the users to be the ones to make decisions around how to manage their devices. We’re not trying to be centralized security for all citizens. What we’re trying to do is empower citizens.” *– NYC Cyber Command Senior Advisor Mitchel Herckis*

In other words, cybersecurity is no longer just a public good; it’s a public necessity. Governments bear a responsibility not only to protect residents on the street, but also in the digital world. Some states and localities have already embraced this responsibility. They’ve turned to next-generation, machine learning-based, on-device mobile security to protect the public’s data and ensure their digital sidewalks are as secure as possible. Their example provides a roadmap for how other government organizations can do the same.

Protecting Constituents: Current Mobile Security Threats Affecting the Public

There are more than 294 million smartphone users in the U.S.,[3] but organizations of all sizes still grapple with how to strengthen mobile security. This challenge is particularly pronounced in state and local government, where constituents are increasingly interfacing with government via digital channels.

Twenty-five percent of government organizations say they’ve experienced a mobile-related security breach in the past year.[4] Nitin Bhatia, chief strategy officer at Zimperium, a leader in enterprise mobile endpoint protection and mobile app protection, says all state and local governments face mobile security risks, including application, network, device and phishing-related threats.

“There are several network threats, including man-in-the-middle attacks, where someone could be listening in to your conversation. There are also a whole lot of application-oriented threats out there, but phishing is the key one that has emerged over the last year,” Bhatia says. “Given the small screen and people’s lack of awareness, a lot of people end up clicking on malicious links.”

Rogue Wi-Fi networks have become more prevalent, Bhatia adds. Through this attack vector, hackers illegitimately set up a Wi-Fi access point within a secure network. When an individual then connects their device to this access point, they unknowingly expose their personal data to hackers as they surf the internet.

Malicious applications and phishing-related mobile security threats pose a range of security, financial and safety risks for constituents. Phishing and hacking can result in banking fraud, financial theft and the loss of sensitive, personal data.

In addition, many constituents struggle with cyber hygiene for their mobile devices. Most devices either do not have the latest security updates or cannot be upgraded due to hardware limitations. With a barrage of OS and app updates every day, it’s almost impossible to keep everything up to date.

All these factors leave mobile devices highly vulnerable to sophisticated attacks resulting in data theft.

Combating Constituents’ Cyber Risks: Case Studies from States and Localities

New York City: Balancing Privacy and Cybersecurity for 8 Million Constituents

New York has made significant investments in digital safety for several years. In 2017, the city founded NYC Cyber Command, a centralized government agency that leads the city’s cybersecurity defense initiatives and works to protect critical public infrastructure from hackers.[5]

The city has sought to increase the security of public internet access points after unsecured public Wi-Fi kiosks contributed to security breaches on residents’ phones. Though the city had already adopted measures such as a DNS filtering solution that helped filter out malicious websites and prevent some attacks, leaders wanted even more robust coverage. So the city worked with one of its technology partners to create a custom mobile application that provided on-device security.

“The internet is a dangerous place in some instances. So by offering the necessary tools, we can expand access [to residents] while helping them be a bit safer online,” says Mitchel Herckis, senior advisor for NYC Cyber Command.

In 2018 the city launched NYC Secure, a free app that gives New Yorkers advanced mobile threat protection capabilities and alerts residents to phishing attempts and unsafe Wi-Fi networks and apps.

Herckis says the city was specifically looking for a security solution that could reduce the risks of phishing and malware, particularly on Android devices since that operating system is open sourced and not as closed as Apple’s iOS operating system.

“We wanted users to be the ones to make decisions on how to manage their devices,” he says. “We’re not trying to be centralized security for all citizens. We’re trying to empower citizens.”

With NYC Secure, users can download the app on their device and it essentially acts as a security overlay on their phone. If a user tries to connect to a rogue Wi-Fi network, for example, they’ll get an alert about this security risk. Android users also get notifications about potentially malicious applications. All of these detection activities take place on-device, meaning data never leaves the device or is transferred across the network via the cloud, which can heighten security risks.

NYC Secure provides all these capabilities without collecting any personal information from users. Herckis says so far the app has 180,000 downloads.

"That's 180,000 less risks of victimization of New Yorkers by hackers," he says.

Los Angeles County: Protecting Public Wi-Fi and Promoting Digital Equity

With a population of more than 10 million, Los Angeles County has more people than most states. Protecting all those residents is difficult by any measure, but keeping constituents safe online is especially challenging. In recent years, L.A. County has expanded public Wi-Fi access, including on its entire fleet of buses, enlarging the cyber threat environment even further.

The county created its own DNS service to protect residents. But depending on the device residents used — and their online behavior — the county still faced security gaps, according to Douglas Anderson, senior director of digital strategy and innovation for the Los Angeles County Metropolitan Transportation Authority.

"People were doing things that would really make them prone to security breaches and get malware on their devices," Anderson says. "That presents a risk because they're using the same channels to access our public services."

While the county's DNS filtering service provided coverage for network-related threats, Los Angeles needed greater security for initial connections from client servers. And IT leaders wanted on-device security that would protect both Apple and Android phones.

The county chose an on-device security solution that it has integrated into its LA Metro Transit Watch app. That app feeds directly into the county's security center, and residents can use it to report security and safety issues on public transit.

Agencies must adopt security technologies that not only advance digital safety, but also increase constituents' knowledge about cyber threats, Anderson says. This approach can also build constituents' trust and ease their privacy concerns when they're using public Wi-Fi or trying to access government services online.

"It raises their awareness and consciousness of security in the first place," he says. "And that's very powerful."

Michigan: Protecting Constituent Access Across the State

Following the success of New York City and Los Angeles County's programs, the state of Michigan implemented its own initiative, Michigan Secure, in early 2021. Former state Chief Security Officer Chris Derusha, now the federal chief information security officer, explained his push for the program in testimony to the U.S. Senate

> "A lot of organizations are starting to adopt more public WiFi since COVID. If that's something we can help facilitate with a commercial product that everybody uses while they're traveling on our networks, then that's just another way for them to gain access and be protected."
>
> *– Douglas Anderson, Senior Director of Digital Strategy and Innovation for the Los Angeles County Metropolitan Transportation Authority*

Homeland Security Committee. Derusha told Congress the program will benefit state and local agencies in Michigan, as well as education institutions, small businesses and underserved communities.

“While the security of government entities, be they state, local or otherwise, is important, our digital ecosystem is ultimately made up of individuals,” he testified. “Every year, the theft of personal information from Americans, including Michiganders, costs our economy billions of dollars. To combat this dangerous trend, the state of Michigan is exploring options to provide greater protections for our residents. This could include a free mobile app that would help residents secure their mobile devices from cybercriminals, reducing the potential of fraud. The app is designed not only for security but for privacy, collecting no identifying information and even receiving the approval of the ACLU. By helping our residents become more secure, we help all levels of government become more secure as well.”

The increasing prevalence of smartphones and other handheld devices has drastically expanded the threat landscape states must secure, says Michigan Chief Information Officer and Department of Technology, Management and Budget Director Brom Stiblitz.

“Our reliance on mobile devices has been met with a surge in activity by cybercriminals looking to access those devices to steal our personal information, and possibly much worse,” Stiblitz said in a press statement. “The Michigan Secure app is a huge step towards protecting Michiganders from these criminals and giving us all some peace of mind as we use our phones and tablets.

Best Practices for Securing Digital Sidewalks

The pandemic forced governments to embrace digital platforms. Now they must ensure those platforms are protected. State and local governments should consider adopting a next-generation, on-device mobile security solution that provides enhanced data protection for constituents without compromising user privacy.

On-device security is essential because it ensures sensitive personal data doesn’t have to go through the network — it never leaves the device.

Government organizations should also look for a machine learning-based solution that helps them keep up with increasingly sophisticated, fast-moving cyber threats across all the key (DNAP) vectors. An artificial intelligence, machine learning-driven solution is critical because it automates threat detection. It can also monitor deviations to the mobile device’s operating system statistics, memory, CPU and other system parameters, and accurately identify the specific type of malicious attack and other specific details related to a security incident. An especially advanced solution may be able to detect as many as six million threats per day.[6]

“The bad guys are using state-of-the-art technology to aggressively go after people’s devices. We have to protect ourselves, and if we don’t have good state-of-the-art systems we’re probably going to fall victim to them very easily,” Bhatia says. “AI and machine learning help you create a real-time solution and protect against fast-moving attackers.”

With the rise of remote work, distance learning and increased digital government services, enterprise mobile security has become essential for state and local governments to secure their digital sidewalks. Just as these organizations focus on physical and public safety, they now must be laser-focused on digital safety. An on-device enterprise mobile security solution can help expand digital access and promote digital equity without significantly raising constituents’ cybersecurity risks.

“Increasingly, we all live our lives online,” Herckis says. “So it’s important that we’re able to help citizens be secure in all aspects of their lives.”

This paper was written and produced by the Center for Digital Government, with information and input from Zimperium.

Endnotes:

1. *www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html*
2. *thehill.com/opinion/cybersecurity/527494-its-time-to-secure-our-digital-sidewalks*
3. *www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/*
4. *www.verizon.com/business/content/dam/resources/reports/2021/2021-msi-public-safety.pdf, p. 5*
5. *www1.nyc.gov/site/cyber/about/about-nyc-cyber-command.page*
6. *https://blog.zimperium.com/malicious-wifi-connections-the-other-mwc/*

Produced by: CENTER FOR DIGITAL GOVERNMENT

For: ZIMPERIUM®

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

Zimperium, one of the global leaders in mobile security, offers the only real-time, on-device, machine learning-based protection against Android, iOS and Chromebooks threats. Powered by z9, Zimperium offers the most complete protection for mobile devices and apps against device, network, phishing and malicious app risks and attacks. Headquartered in Dallas, TX, Zimperium is backed by Warburg Pincus, SoftBank, Samsung, Sierra Ventures and Telstra Ventures. Learn more at **www.zimperium.com** or our official blog at **https://blog.zimperium.com**.

IMAGES PROVIDED BY SHUTTERSTOCK.COM