Update: Cybersecurity Challenges, Solutions Grow with Telework Shifts

One month on, mobile device security and video-teleconferencing platforms enter the spotlight.

James Mersol
Mon, 04/06/2020 - 12:38

Despite initial challenges to telework for some, most public and private organizations have adapted well to the new normal, setting up routine meetings to address any questions some may have and ensuring that most can access the resources they need to achieve their mission.

Photo Credit: Pofuduk Images/iStock
One lesson learned is that “organizations are not a monolithic entity,” said John Dickson, principal at Denim Group, a cybersecurity consulting firm based in San Antonio, Texas.

Teams whose work lent itself well to working from home have adapted with few hurdles to new processes. Other functions that required physical interaction — notably including finance and procurement — have faced greater challenges. Many financial processes require physical signatures and other measures designed to mitigate risk of fraud or embezzlement, which cannot function in a fully remote environment. While there are some alternatives, like DocuSign, in the interim some agencies are postponing purchasing orders or designating small teams of essential personnel to carry out these critical duties in person.

As organizations shift their routines and methods, threats to cybersecurity have shifted to exploit potential vulnerabilities in the relatively new paradigm. Cybersecurity continues to evolve to meet the challenge.

For remote employees, security leaders are continuously updating remote security measures for devices. Amid the shift to mass telework, the National Institute of Standards and Technology (NIST) revised its 2013 guidelines on enterprise mobile device security with a wide range of new measures to protect both organization-issued and personal mobile devices.

Mobile device management was "all we had" in 2013, said Tim LeMaster, director of systems engineering at Lookout, a mobile security firm adding that the measures outlined in NIST’s guidelines, from mobile threat defense to mobile application management, demonstrate the need to implement a “layered defense” of mobile security options.

“There is no one solution to all mobile threats,” LeMaster said.

The guidelines are important not only for increased individual cybersecurity during the pandemic, but also because even beforehand, mobile devices had outpaced personal computers as the business device of choice. Additionally, mobile devices are exposed to a higher number of threat vectors, including phishing texts and malware embedded in applications.
“To reduce risk to sensitive data and systems, federal enterprises need to institute the appropriate policies and infrastructure to manage and secure mobile devices, applications, content and access,” the NIST draft publication states, recommending that organizations should develop a risk management plan for all devices that connect to their networks, employing a range of solutions to defend against potential threats.

NIST’s draft guidelines are currently open for public comment through June 26.

As the vast majority of organizations have moved to video teleconferencing to stay connected while working remotely, the risk surrounding those platforms has increased as well. The popular platform Zoom, which has become the host to scores of webinars, public- and private-sector meetings and groups of friends meeting up online for drinks, games or conversation, has faced particular scrutiny. On April 1, after it was revealed that Zoom does not actually offer end-to-end encryption as the company claimed, Zoom CEO Eric Yuan wrote in a company blog post, “over the next 90 days, we are committed to dedicating the resources needed to better identify, address and fix issues proactively. We are also committed to being transparent throughout this process. We want to do what it takes to maintain your trust.”

Despite Zoom’s pledge to secure its platform, encryption vulnerabilities are not the only risk video teleconferencing users need to watch out for. Malicious actors have been “zoombombing” calls that openly share their dial-in information or allow any guest to share their screens. The issue is pervasive enough that the FBI’s Boston field office issued a warning to video-teleconferencing users about the attacks, which traditionally involve pornography, hate speech and threatening language, urging victims to report incidents to the FBI’s Internet Crime Complaint Center (IC3) and specific threats to their nearest field office. The office also encouraged users to set video-teleconferencing calls to private, limit access to dial-in links, and ensure video-teleconferencing users
“The problem is, we don’t have a lot of options,” Dickson said, noting that many organizations have either done away with traditional phone conference lines or found that providers simply do not have the bandwidth to support multiple conference lines at once. Other videoconferencing providers, such as Google Hangouts and Skype also lack end-to-end encryption.

The good news, however, is that capability providers and teams in both the public and private sector are continuously adapting to these challenges.

“America has a history of pivoting to innovation in times of need,” said Thomas Ashbrook, senior advisor at PreVeil, a secure communication service, “and this is one of those times.”

As an example of this pivot, both Ashbrook and Sanjeev Verma, CEO of PreVeil, discussed how the mass shift to telework fortunately came at the same time as the ramp up in the defense industrial base toward the Defense Department’s Cybersecurity Maturity Model Certification (CMMC), which provides a rubric for vendors to implement secure communication and other cybersecurity measures.

Verma explained that for companies to work with the DOD, they need to have end-to-end encryption built into their online communication systems. While few platforms currently offer that capability, the demand for end-to-end encryption is growing not only from prospective vendors, but also for public- and private-sector organizations concerned about malicious actors targeting home Wi-Fi networks as a vector.

Other email security providers are recognizing the increased risk of phishing and building in safeguards.

“We’ve seen at least two dozen different kinds of COVID-related phishing,” said Dave Baggett, CEO of INKY, one email security provider.

Seeing the spike in phishing, INKY embedded a banner into its phishing monitoring software that pops up for any email related to COVID-19, directing users to be especially cautious and head to the CDC and WHO websites for the most up-to-date official guidance.
Baggett said that one shift leaving teams open to phishing attacks is the change in daily routines. Even though employees can no longer physically speak to the alleged sender of a suspicious email in the office, he urged anyone who receives a suspicious email to confirm with their colleagues through another channel, such as instant messaging or phone.

“Never do anything on the basis of email alone,” Baggett advised.

*This article is part of a series on *cybersecurity and telework*. Read the first article in the series [here](#).*