COSMOS
Navigate the Compliance Universe

ethikos Volume 34, Number 5. May 01, 2020
Security in the time of COVID-19

By John Nye

John Nye (john.nye@cynergistek.com) is Principal, Cybersecurity Research and Communication, CynergisTek, Austin, TX.

- linkedin.com/in/john-nye-734ba026/

At this moment in time, the world is in a very strange state: More than half the population of the US—and the world—has been asked or ordered to stay at home. By the time this article is published, it is likely this number will have grown even more. How does this affect security? In many ways, this crisis has caused a perfect storm for security to go spiraling out of control. First, consider the sheer number of people that were forced to begin working from home in 2020. A *majority* of the workforce in the US is now telecommuting. Add to that the millions of students—from preschool through graduate level—that are learning online. Under the best of circumstances, working from home is less secure than working from an access-controlled office. In addition to all the new people working remotely, there are millions of Americans that have been laid off, furloughed, or fired from their jobs. This also entices a much larger portion of the population to turn to less-than-ethical or even criminal methods of making money.

Remote workers

One of the first things to consider is how many of the workers now working remotely had received adequate, if any, remote worker awareness training. In many cases, companies tried their hardest to keep people in the office until the last possible minute. This means they were issuing laptops and kicking people out the door (hopefully with at least a two-factor authentication token for their virtual private network). In addition to no awareness of the possible security issues, millions of workers are now working at home using their consumer-grade wireless hotspots. Consider how many of those are vulnerable or still use default admin passwords. Many of the routers that can be purchased at the big-box stores are riddled with security flaws and default usernames and passwords to access the administrative settings of the router that can be easily found online. A malicious actor with access to a router's configuration can read all traffic on that network, reroute any requests to anywhere they please, and generally have complete control of the network and any devices connected to it.

The worries don't even begin to slow there, though. What about all the smart devices and digital assistants that remote workers have at home? Most of those devices have microphones that are always listening to and recording potentially sensitive meetings and calls with customers, colleagues, or even patients. In fact, the concerns are staggering with just one surprisingly common type of smart devices—digital assistants, such as Google Home or Amazon's Echo. They are supposed to begin listening only when someone uses the key phrase, but they are passively listening for that term all the time to become alert.[1] Most of the phrases can be mistaken (false positive) for other words by the devices, and they are known to record conversations after being mistakenly alerted.[2]

Other smart devices have integrated digital assistants, meaning they have microphones that are constantly listening, too, such as smart TVs with voice control, cameras, or home automation devices. There is myriad other

concerns around internet-connected devices—especially consumer-grade products—but this is the tip of the iceberg.