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.

Growing criminal population

To begin with, all the people that make money from physical theft or other means that require in-person interaction with people are as out of work as the retail and food service industry workers. The current criminal population is shifting their focus to remote attacks like phishing, wire fraud, and countless other internet-based attacks. Amid crisis, some cybercriminal organizations have announced that they will stop attacking hospitals and other healthcare organizations.[3] However, that might lead the criminals who are just ramping up their online attacks to attack healthcare organizations. In the corporate world, the regular groups of cyberattackers, as well as the newcomers to the game, are going to be putting more focus on businesses.

There are other millions of people that have lost their sources of income—not to mention students with lots of spare time and internet connections—who might be getting, or might get, desperate and turn to crime. As people turn to criminal activity to make ends meet, they will begin with the lowest-hanging fruit (i.e., the most vulnerable to attack will get attacked first and repeatedly). The longer this crisis goes on—and the longer the economic effect of it lasts—the more previously law-abiding citizens might turn to criminal or at least less-than-ethical actions to make money. The best thing organizations can do right now is ramp up awareness training. However, it will only work if they connect with users around topics and issues that are really close to their current situation, not just send out that ineffective video awareness training so many organizations have used in the past.

Awareness training

Awareness training, which can be difficult to conduct effectively, is more important now than ever before. As we all know, the vast majority of people working from home are doing so in less-than-ideal circumstances, with all the kids being home, needing snacks and help to do their online schoolwork. There is also a very large population of workers that don't typically work from home. Finally, consider that everyone's internet is slower than it was, partly because so many more people are online, and partly because more devices are connected to Wi-Fi.[4] Couple those distractions and issues with weak security measures in the form of consumer-grade wireless routers, insecure software, often outdated hardware, and no corporate firewall, and the security risk starts growing almost exponentially.

However, this strange situation means that everyone is a captive audience now, stuck at home doing the same tasks over and over, so anything that breaks the routine, such as mandatory training, will likely get played. But, do keep in mind that all the distractions make the chances that the remote workforce will pay attention to the training even lower than normal, which can be pretty abysmal. The trick is to make it something they *want* to listen to and absorb. Security is rarely an enthralling topic to the noninitiated, and it generally brings fear along for the ride, which is the last thing the world needs more of during a pandemic. So, how does one reach the audience that is essentially working against them? The answer to this seemingly daunting question is shockingly simple: Make it personal.

Make it personal

The fact that most people are working from home and are at a greater risk of being targeted for cybercrime actually presents a unique opportunity to personalize the awareness training. Begin by presenting in a personal way. Talk about how the threat is to *their* accounts, *their* money, and *their* network at home. This alone will catch people's attention and begin to draw them in. Take it further; don't start off with a legalese-riddled monologue

about how corporate interests will be protected by these measures. Since even the most dedicated employees may care more about other things when they are at home than the corporate "family," make sure the awareness training your organization presents reflects this reality. Tell them how their bank and social media accounts can be at risk—even when their child borrows a device to play or attend a class. If the same awareness training that has always been given was simply rewritten to leave the corporate part for the end, people would not only pay attention, they would ingest the information, remember it, use it, and even pass it along to their loved ones. Of course, there is likely some requirement to do mandated awareness training in many organizations. This is a good time to remember that these are mostly designed to satisfy some compliance, regulatory, or even policy requirement and are rarely good for more than checking a box.

Monitor everything closely

In addition to getting telecommuters aware of the risks and threats to them and corporate assets, the corporate security should still be at work, and the security/network operations center should be especially vigilant, monitoring accesses, data movement, malware, etc. They should all be working remotely but still have access to their security information and event management feeds and other data feeds. The more simplistic and basic attacks (especially those coming from new criminals) are pretty easy to spot and thwart from a monitoring standpoint. The problem is that those who are monitoring those feeds have the same distractions and potential security holes in their home network as everyone else. So, make sure staffing is appropriately modified to meet the combination of demand and distraction.

A time of national crisis is not the time to do hiring freezes in security and information technology (IT) departments; if anything, it is time to ramp up hiring. It is also not the time to postpone patches and vulnerability scanning; it is time to step up to the best practice level most organizations have been trying to get to. Many modern vulnerability scanners can put an agent on remote computers that will do basic scans of the network they are connected to. If these can be done with the permission of the network owners/maintainers (the employees working remotely), they should be done. Even the most basic security scans on a home network will point out the most glaring and dangerous issues, and IT or information security can walk the affected employees through fixing the issues before they are exploited.

Conclusion

The declaration of a national emergency has resulted in millions of people working from home and students attending schools remotely. This includes many criminals, as well as millions more who are out of work and have the potential to get desperate and become criminals themselves. The people working from home have little or no cybersecurity awareness training, and there has never been a time when it could make a bigger difference. In addition, people are now doing sensitive corporate work and conducting meetings in inherently unsafe environments. All of these factors, as well as other worries, have set the stage for massive digital attacks.

Organizations can try and get ahead of this impending trend by better informing their employees through personalized awareness training. They can also ensure there is still budget to grow and bolster the security and IT teams as this crisis looms on. Employee awareness and security's attention to detail may be the only way to survive this time without any major breaches.

1 Molly McLaughlin, "What a Virtual Assistant is and How it Works," Lifewire, January 29, 2020, https://bit.ly/2JYIvgY.
2 Sara Morrison, "Alexa records you more often than you think," *Vox*, February 21, 2020, https://bit.ly/2V71HiZ.
3 Bradley Barth, "Some cybercriminals consider laying off health care targets amid COVID-19 crisis," SC Media,

March 19, 2020, https://bit.ly/34yuO1A.
4 Davey Alba and Cecilia Kang, "So We're Working From Home. Can the Internet Handle It?" *The New York Times*, March 16, 2020, https://nyti.ms/2V69MEt.