COVID-19 Probably Broke Your Organization's Telework Cyber Policy. Here's How to Fix it

By Daniel S. Marvin

If you are like many Americans, you are probably reading this as you telework from home while weathering the COVID-19 storm. It is also probable that your organization has some sort of a telework cybersecurity policy, either as a limited part of its greater information security program, or one that was hastily put together in response to the pandemic. In either circumstance, there is a good chance such policy is insufficient and will not withstand scrutiny as data breaches occur and insurance claims and lawsuits follow. To be sure, the obligations of organizations to have a risk-based and reasonable cybersecurity policy did not change with the arrival of COVID-19. However, new risks have arisen, and what may be considered reasonable has changed. For example, many cybersecurity regulations and best practices require such things as an asset inventory, device management, access controls, identity management, systems security, network monitoring and physical security. In the telework era, how those practices need to be dealt with from a security perspective have raised many questions which must be addressed. For example, does an asset inventory need to include employees' home computer and mobile devices? Do employers need to consider the physical security of where its employees use and store their technology? Look around your environment now. Is Alexa listening in? Does your laptop's webcam have a cover? Do you have home security cameras that are recording your screen (and you)? Maybe you have a smart TV in your home office. Is that listening to you? Is your Wi-Fi network secure? Are you printing documents? These questions are enough to drive IT managers and CISOs crazy, but they must be addressed and documented in a proper telework policy; make no mistake, when the insurance claims and lawsuits start to happen – and they will happen – insurers, regulators and attorneys will put your organization's telework practices and written polices under a microscope.

There is no doubt that businesses are in an unenviable position. In a rush to move entire workforces mobile, there was not enough time to give due consideration to the cybersecurity needs of mass telework. Some organizations rolled out entire software infrastructure changes without beta testing, while others failed to pay close enough attention to how technology changes could alter their risk profile and how those risks could be effectively mitigated. It has certainly been an unprecedented time, and few businesses can be blamed for making the perfect the enemy of the good. But as time passes and we settle into a new normal, the grace period, if there ever was one, will come to an end, and it is time for all organizations to create, review, and revise telework policies. For those that aren't sure where to begin, keep reading.

In 2016, the National Institute of Standards and Technology (NIST) issued the NIST Special Publication (SP) 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.* Publication SP-800-46 was designed to help organizations mitigate security risks associated with the enterprise technologies used for teleworking, such as remote access servers, telework client devices, and remote access communications, and provides a good roadmap for organizations to follow. Last month, NIST's Information Technology Laboratory issued a bulletin reiterating that the recommendations of Publication SP 800-46 are still relevant today. Publication SP 800-46 is a great place to start in to create or revise a telework policy, but there are some important operational factors for IT teams to account for in light of the pandemic which were not (and could not have) been contemplated by NIST in 2016.

The core of a telework policy, as NIST advises, should define which forms of remote access the organization permits, which types of telework devices are permitted to use each form of remote access, and the type of access each type of teleworker is granted. For companies with existing written telework policies, these considerations will likely need to be broadened so that employees are not in violation of restrictive policies which were not drafted with the intent of moving an entire workforce to home-based work. Importantly, these polices should be carefully documented. In addition, NIST advises that as part of creating a telework security policy, an organization should make its own risk-based decisions about what levels of remote access should be permitted from which types of telework client devices. For example, according to NIST, an organization may choose to have tiered levels of remote access, such as allowing organization-owned computers to access many resources, BYOD computers to access a limited set of resources, and BYOD mobile devices to access only one or two lower risk resources, such as webmail. As NIST suggests, having tiered levels of remote access allows organizations to limit the risk it incurs by permitting the most controlled devices to have the most access and the least controlled devices to have minimal access. This is sound advice, and again, any tiered access should be carefully documented.

Perhaps the most important recommendation of Publication SP-800-46 is that organizations plan telework-related security policies and controls based on the assumption that external environments contain hostile threats. In particular, NIST suggests that organization should assume that malicious parties will gain control of telework client devices and attempt to recover sensitive data from them or leverage the devices to gain access to the enterprise network. While this assumption may have always been the case, organizations, in many cases, have now lost physical control of all, or virtually all of devices being used by employees to their networks. Telework polices which were designed to address a handful of remote workers, laptops or external devices, now need to adapt to address connected devices in the hands of all employees in different physical locations. Add to that the security challenges posed by the home environment, such as virtual assistants and unsecured Wi-Fi networks, and we have nothing short of a reimagining of what a successful cybersecurity policy need to look like.

IT departments are now dealing with unprecedented circumstances, and the thoughts here only present the tip of the iceberg. And like an iceberg, most of the IT infrastructure necessary for a

good telework policy lies beneath the surface; the work is not easy, but vital. The details of endpoint security, VPNs, firewalls, encryption, tiered access, multifactor authentication and a host of other things need to be addressed and fine-tuned, and of course documented. Because what should be on the surface for all to see (especially those regulators, lawyers) is an effective written telework policy designed for the times. As a final note, as with any cybersecurity policy, employees are on the front line while teleworking, so training is key. Stay safe. Stay healthy. Stay secure.