**Phyllis A. Schneck**
Associate Editor in Chief

# Cybersecurity During COVID-19

The COVID-19 pandemic has blended our work and home environments, expanding and tangling the cyberattack surface. More than ever, company vulnerabilities can be heightened by employee personal electronic security vulnerabilities. Outgoing Editor in Chief David Nicol, and his incoming replacement, Sean Peisert, both wrote editorials on this topic in the immediate past two issues. A key message from Nicol is the critical role of cybersecurity and the dependence on it as a pandemic moved a global economy into a world of information traveling in the form of bits of light. A key message from Peisert is what the cybersecurity community brings to our endurance and eventual safe return to the world we knew.

Building on these themes, as our professional and social worlds converged into the home with the proverbial bookcases in the background of the laptop camera, the boundaries between work and home became more flexible. We recognize this in the long hours, our commutes replaced by earlier and later conference calls, the opportunity for all to learn the names and sounds of our colleagues' pets over Zoom, and also the chance to see or FaceTime more of the little ones in the family who can find a light in this pandemic on Disney+.

However, more subtly, as the chief information security officer (CISO) of a large company, I and my colleagues in this space are constantly evolving, varying directly with attack surfaces, threat pictures, and company priorities to mitigate risk. Networks are amorphous and have no static shape. Balancing technology, regulatory obligations, process, funds, and people all in the name of managing risk to protect the business, customers, and employees, I view the current environment as beckoning a more flexible concept one could call *adaptive security*, a term we began to use—if not coined—back when I was applying high-performance computing to cryptography at Georgia Tech. Security needs to be applied as needed and in the way it is needed, always ready to pivot.

Applying this to the current environment, I view the pandemic-driven disappearing work–home boundaries as an expansion of the cybersecurity attack surface and thus as continuing to change the shape of the protected surfaces in two ways. First, as noted by countless others, the home office, or better yet, the living room-turned-home office, was never designed to support phone calls and video conferences, much less productivity and protection of proprietary information. However, it was rapidly converted into exactly that in mid-March, including the personal communication devices that answer questions or play music when you call their name (now ubiquitous in our homes), and entire households simultaneously sharing the same network on which work will now depend, whether or not the encryption has been updated to a modern strength. We have addressed many of these areas in *IEEE Security & Privacy* and in other fora, so this discussion will expand on the second way that the cybersecurity attack surface has been expanded: our personal electronic footprint.

As cybersecurity professionals, we must protect the cybersecurity of our companies and employees, while continuing to strive for excellence in the business. In our current environment, we should proactively address vulnerable and relevant areas of employees' personal electronic footprint. Our main role is to protect and defend the electronic assets of our company. However, a key vector to penetrate corporate electronic assets is through our employees via their personal devices, email, and other connectivity—even without the connectivity that uses simple social engineering. With escalating cyberthreats accompanying a year that has

*Digital Object Identifier 10.1109/MSEC.2020.3019678*
*Date of current version: 29 October 2020*

 

brought us fires, earthquakes, early hurricanes, locusts, global sickness, and a pending asteroid, it is our responsibility to educate and provide our employees with information, training, and, as needed, office equipment to prevent adversaries from taking advantage of an environment that has employees intermixing their personal space with work space.

Security executives can benefit employees and our business by encouraging our workforce to have strong encryption on their home routers, use strong passwords on personal accounts, and be more guarded than ever with personal information (most places that ask for it do not need it and cannot require you to provide it). We can point to free downloads for home use of the endpoint security that we have selected as a company so it may be used in lieu of other products that are offered "free" in big stores but often provide less protection. We can encourage our employees to send any suspicious, targeted emails received on a personal account to the company for 1) assessment or 2) an understanding of who is potentially maliciously targeting our employees. Cyberadversaries may launch malware into the personal email or web browser of a "home user" to capture access to the personal device(s) and gain information that the particular adversary may find useful to lead him or her to company proprietary information. Further, an adversary could use that access to capture login credentials and abuse the person's name, identity, or reputation, which spills over to the corporate reputation in severe cases or with high-profile employees.

I would suggest to all information security executives to put the power of company information security and privacy regimes to help our employees protect their remote and personal electronic space to the best of our abilities while still ensuring that these benefits do not encroach on the privacy of employees' personal information.

The role of a CISO in a pandemic-driven, instantly long-term remote workforce must continue to be agile and fiercely protective but should expand to offer insights and assistance in ensuring some training, awareness, and cover for the personal electronic footprint during these challenging times.

*IEEE Security & Privacy* has a key role to play in bringing together the top technical research and the best privacy thinkers to offer a forum for ways our passions can assist the community. The lines between corporate and personal electronic security are gone with our sudden but long-term remote work infrastructure. We need to extend our best and brightest to offer to protect parts of the personal electronic footprint for employees. People are our most precious asset, our well-being, and our way of life. That is why we actually do this security and privacy stuff anyway. In closing, I want to offer a warm welcome to Sean Peisert and use his words in this similar context: "for those security and privacy professionals who can, please join me."





*Digital Object Identifier 10.1109/MSEC.2020.2981218*