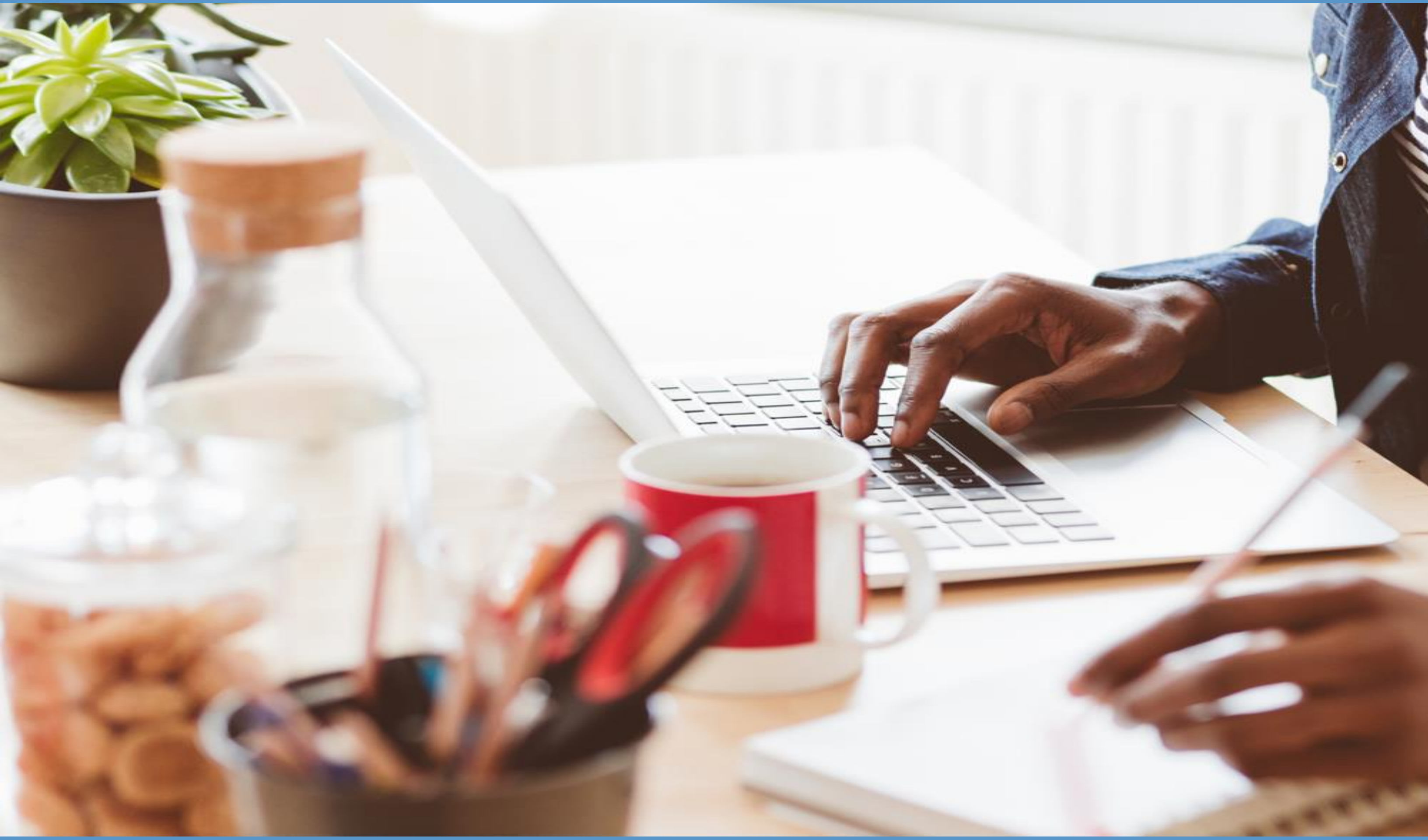


Why WFH Is Different Enough to Be More Dangerous

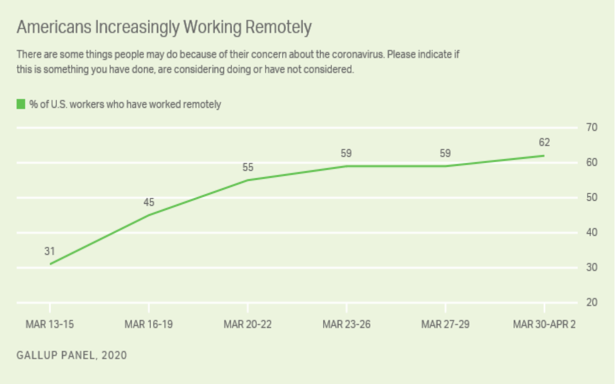
WHITE PAPER

cyberconIQ

Why WFH Is Just Different Enough to Be More Dangerous

By Dr. James Norrie, Founder & CEO

Given the massive lock-downs associated with Covid-19 that occurred around the world this past spring, many employees are now working from home, either part time or full time? Of course, working from home is not new, as almost 31% of employees were already doing so when the coronavirus emerged. The only astonishing part is the scale, which saw a doubling of this in four weeks:


Americans Increasingly Working Remotely

There are some things people may do because of their concern about the coronavirus. Please indicate if this is something you have done, are considering doing or have not considered.

GALLUP PANEL, 2020

So, what is different – and just different enough to be dangerous in our view – is not the sudden scale of the WFH phenomena; but rather how it affects the *"clues and cues"* your employees react to while working from home. What is different is the environment of work rather than its content. As that base context changes, so does your company's overall protect it.

Let us consider a few basics: if work is a destination as exhibited in the phrase "going to work", then we arrive at a place that is designed for that context. It may have had specific hours, fewer distractions, and the fact there was often a range of tools, policies and practices we associated with the environment we were in and the equipment used. This includes computers that were provided specifically by the employer and for work purposes. In this context, work is **place-based**. As cybersecurity professionals, it was our job to secure the workplace by letting our employees in and keeping the bad guys out. We enabled authentication of users at work and then provided whatever they needed to do their work inside that perimeter. Fairly simple right? Or at least easily understandable as a security assignment that we executed well against.

Now, consider what happens when the context of work changes to being done from home. A lot changes as work is now **activity-based**. Work may be done from anywhere the employee is, home or elsewhere. Employees may be doing it on work computers, home computers or other digital devices. Again, this is not particularly new because cybersecurity professionals have been adapting to BYOD ("bring your own device") to work for years, even if they did not exactly love the idea. Remote users have tunneled into corporate systems using VPN's and similar tools forever. Aspects like this offer a new security paradigm: everyone is now outside work and our job is to let them in. They want remote access to everything they use to have inside the perimeter in a fast, efficient and effortless way remotely. Unless we can seamlessly provide that quickly, we risk the creativity of the user stripping away our well-worn and previously workable security policies and procedures.

Validation of this can be found in Tessian's most recent "The State of Data Loss" report. It notes 88% of successful data breaches are caused by human error while concurrently finding that, even while they are aware of that risky fact, 52% of those same employees believe they can get away with riskier behavior when working from home because of the lack of security oversight and policy controls imposed. In other cases, employees may not be willfully ignoring known security practices, but face constant distractions and interruptions that alter the flow of their concentration when working. Either way, as IT professionals, the critical conclusion is that WFM for most of us is psychologically different.

Once again, the problem is not a technology problem but a human problem. As employees settle into the comfortable environment of home while conducting work, their online security profile naturally changes. While we may provide a laptop and VPN access for secure remote access to corporate networks, that does not connect them psychologically to work. It only takes one unintended click to unleash a torrent of regulatory, financial and legal harm on us.

At cyberconIQ, we measure an employee's base instincts about how they behave online and improve their understanding of how that makes them vulnerable to online threats. We believe deeply that the solution lies in a greater understanding and self-awareness of these to improve enterprise security outcomes. By focusing on that last mile of your human firewall – no matter when or where you may be working from – we enhance an individuals' ability to see threat contexts and it works.

For example, the last three months have seen an incredible spike in both the sheer volume of social engineering and business e-mail compromise attacks and their reliance on tapping into the anxiety and feelings of dislocation and isolation that the coronavirus pandemic has unleashed globally. One way to approach this problem is to provide a steady diet of updates, content alerts and advisories about the latest trickery being unleashed on your employees to keep them on guard. That approach creates fear, albeit a low level of fear because with each additional alert or advisory, fatigue-based complacency sets in and we start to get the opposite impact to what we seek to achieve: we are reducing awareness and have induced a state of hypervigilance, something I describe in great detail in my latest book. If that is all we can do as cybersecurity professionals – sling fear – we are not doing a great job.

Instead, we must focus on the context of attacks and how to equip employees to predict, detect and interdict their actions in the face of an avalanche of evolving content-based attacks. We must educate them about how to avoid personal behavior that is risky, regardless of the content used to provoke it by those trying to compromise us. This involves more than simple rules, or the rote memorization of current campaign themes. Instead, we must learn to adapt our personalities – our base instincts and impulses all of which are uniquely individual - to this different work environment. This requires helping employee adapt responses to the embedded cues and clues of working from home to spot and avoid these new risks. This new approach makes them willingly to comply with new ways of doing work, partnering with the company's IT, security and risk professionals to make "cybersecurity a team sport", no matter what position on the team they play and whether they are playing an at-home or an away game. What is the net-net of this new normal? We think it means changing their psychology not just their technology – the surest path to making us all safer online while working from home.

For more information be sure to check out both our website and our book. Both contain a plethora of research and facts to why our company is doing cybersecurity right.

For more information or to learn more about the cyberconIQ solution, please contact us at info@cyberconiq.com