The WFH environment and associated data risks: A new perspective

The COVID-19 pandemic changed the landscape of the corporate world drastically. Lockdown, shelter-in-place orders, bans on gatherings for safety purposes and national and international travel restrictions meant the world, and businesses, couldn't function as they were doing in the pre-pandemic times. Tradeshows went online, meetings happened from the couch in the living room, company parties meant saying cheers and sharing a glass of wine over a Zoom call with your video turned on. The transition to this work-from-home (WFH) culture on such a large scale and at this level was unforeseen, but it has happened nevertheless. While initially there were talks of this transition being short-lived and people resuming 'normal' lives in a couple of weeks, now it is clear that this model is here to stay. Organizations and employees alike are seeing the numerous benefits of working from home.

From the company perspective, three big benefits stand out: they include saving significantly on real estate expenses--with staff working from home they don't have to spend as much on renting office space, an increase in productivity, and a drop in absenteeism and employee turnover.

From the workforce perspective, a lot of people are happier working from home as it helps cut the travel time to work and also supports better work/life balance. There's a lot of flexibility, which is appreciated by employees with children or elderly parents who require caregiving.

In light of these benefits for both parties, it is highly unlikely that we will ever go back to the traditional office setup. What is more likely to take shape is a mixed environment where employees are mostly operating remotely and perhaps stepping into the office once in a while for catch-up sessions. As homes expand to accommodate office space, traditional office spaces will shrink to include probably just a conference room for in-person meetings. While this makes perfect sense, there's something here that you can't ignore- Data security. WFH may keep your staff safe during the pandemic, but it may put your data at risk and jeopardize your data security if you don't take the right precautions. Why? Because WFH often involves employees using their own devices for work purposes and that blurs a lot of boundaries. It also raises several questions from the data security perspective which makes it imperative that you have mechanisms in place to mitigate possible data loss, leak, or misuse before you allow employees to use their own devices for work purposes. There are multiple risks associated with the WFH environment. Some of them include

Restrictions on installing firewalls, antivirus, system/software updates, and security patches

When your employees are in the office physically and using your computers, you can install firewalls and access control mechanisms. For example, you can block non-work-related sites or sites with 3rd party cookies, or set up password policies for them to follow when using the device, etc. But, if they are working from home and using their own devices, there's no way you can install firewalls or have access restrictions like that in place at the system level. Similarly, you can ensure your work computers are up-to-date in terms of security patches, system updates, and software upgrades, but you can't force an employee to install security patches or antivirus on their PC at home!

Keeping your data safe after an employee quits

When your employees are working from home using their own devices, how can you be sure you recovered all your data and erased them permanently from your former employee's devices? How do you ensure they don't have a copy of the sensitive information stored somewhere that could be misused intentionally or unintentionally cause a data breach.

Safeguarding access to your data in case of unexpected events such a device theft or breakdown

If your employee is using their personal device for work and it gets stolen, how do you handle the data loss and any data compromise that could possibly follow. Similarly, if something goes wrong with their device, how do you ensure your data is not lost and your work is not stalled? Also, if the device goes into repair, how can you be sure of the security of your data then?

Challenges brought on by device sharing

If your employees are using their own devices for work purposes, you can’t stop them from sharing their devices with friends and family. But, device sharing can put your data at risk of being stolen.

Remember WFH is not necessarily just WFH

When we use the term, WFH, the first image that comes to mind is of a person sitting in their living room or home office desk and working on a laptop. But, remember that’s not necessarily true. When you follow the WFH model, it enables your employees to work from anywhere! The recent ‘workation’ (work+vacation) trend that’s catching on is a testimonial to this fact. For all you know, your employee may be working from the Starbucks two states away, or they may be at the airport sending that last report in before they take off for a vacation, or they may dial into that important meeting from the resort they are staying at--all instances where they may be using public Wi-Fi networks, compounding the risk to your data from cybercriminals

Let’s face it! The WFH environment coupled with the BYOD (Bring-your-own-device) makes organizations much more vulnerable to cybersecurity threats than the traditional office setup. However, that doesn’t mean there’s no solution. As a company, you can still put various mechanisms in place to ensure the safety and security of your data. You should also train your employees on how to safeguard themselves and your data from cybercriminals. A managed service provider (MSP) specializing in cybersecurity, data backup, and recover can help you with both of these. They would know what tools you can use to keep your data secure even in the WFH scenario and they will also be able to train your employees on the common mistakes that people make unwittingly which often leads to major data breaches.

For more information please contact,
Sharon Peralta | Chief Technology Strategist | Essential Tech Solutions
Phone: 207-324-4485 | Email: Sharon@etechsolutions.me