



IT Pro Portal

Technology's role in improving work-life balance for remote workers

The ability to work remotely has become a selling point for some organisations as more employees demand it.



As communication infrastructure has improved (with the amount of homes with superfast broadband connections topping [10.8 million last year](#)), workers now receive an almost identical connectivity experience at home as they do in the office. Because of this, a rising number of young professionals are working remotely and living a nomadic lifestyle. The trend shows no sign of abating either, with the World Economic Forum calling remote working [“one of the biggest drivers of transformation”](#) in the workplace.

2017 is likely to be something of a tipping point when it comes to remote working, with more than half of businesses in the UK now offering remote working policies according to the [Work Foundation at Lancaster University](#). Now, the ability to work from home is just as likely to be added to a job advert as the existence of a workplace pension or a complimentary gym membership. The trend is likely to continue too, as the same research predicts that by 2020 over two thirds (70 per cent) of organisations will allow their staff to work from home.

Benefits for all

There are advantages from both sides with remote working. For businesses, allowing home working can lead to a rise in productivity. Usual office distractions like water cooler gossip, impromptu meetings and others are no longer an issue. So much so that reports claim that productivity can increase by some **30 per cent**. It can also reduce the need for bricks and mortar expenditure considerably, as less office space is required. In fact, financial behemoth American Express told Forbes that it has enjoyed annual savings of **\$10 to \$15 million** thanks to allowing its staff to work remotely.

However, you need to proceed with caution. It's not simply a case of allowing any employee with a laptop, internet connection and desire to work in their pyjamas the option to work from home. Before you offer them the ability to work from home there needs to be a certain amount of technology investment undertaken to ensure that you mitigate the threat of new and emerging cyber-attacks.

In order to do so, businesses must ensure there is a range of technologies working seamlessly together to provide secure access while not impacting the end-user experience. Security is the key as you don't want your remote users to become the weak link in your cyber defences. It is important to use authentication techniques such as two-factor. The technology ensures that access is only provided when a user meets two separate authentication criteria, often a password and a unique, temporary code provided to their mobile handset via SMS. The good news is that your users are now used to two-factor authentication from when they bank online.

The data between your employee's device (which could be anything from a traditional PC to a tablet or mobile phone) and your organisation's servers must be encrypted whenever they log in. As older cryptography techniques have become easier to hack, connections should now be secured using IPSEC with DES or 3DES. This means that even if a hacker was able to intercept your data, it would be unintelligible. While simple passwords to crack – such as 123456 or password1 – are never recommended, the advice around passwords has somewhat evolved. The National Institute of Standards and Technology **now recommends** focusing on usability and practicality as opposed to an overly complex password that your staff will only have to write down on a Post-it note or their mobile phone in order to remember it.

The need to evolve

Simply allowing your staff to access your network from home as they would in the office, could leave the business systems and networks open to being infected should their laptop or home PC be carrying a virus. The technologies used by remote workers to access the information they need from home has needed to evolve. It is simply not practical to rely on an already beleaguered IT department to secure every single device that remote workers use; therefore, other solutions have become vital.

One solution for example, is to provide a specific cloud-based desktop solution for remote users, which sends a live snapshot of your office desktop to a remote device. If a user clicks or types, these interactions are reflected on the server. This negates the need for applications to be installed on the user's remote device, and provides a barrier to prevent viruses from being transmitted from the remote worker's device back to the corporate network. However, if the user is offline or their connection drops it means they are unable to work.

A better solution is to provide access to all files via a web server through a browser. Because so many devices now support web browsing, this provides many more ways to work remotely. The added benefit is that it will use the SSL (Secure Sockets Layer) protocol to establish an encrypted link.

A distant memory

With the push to work remotely coming from both sides, the traditional work and life balance is becoming increasingly blended. Emails can be sent straight to an employee's device, work can be completed anywhere thanks to laptops, and the days of a simple 9-to-5 existence are becoming a distant memory.

All of these increased capabilities shouldn't be at the detriment of cyber resilience though. Mobile Device Management (MDM) technology has become an imperative tool for IT departments to manage the additional endpoints brought on by the remote working trend, and provides a means to instruct devices to delete any sensitive data should the device become compromised.




Link to the original article:

<https://www.itproportal.com/features/technologys-role-in-improving-work-life-balance-for-remote-workers/>

Wavex Technology Limited

 70 Wilson Street, London

 020 7030 3210

 tellmemore@wavex.co.uk