

# Out of sight, not out of mind

## Securing remote workers using two-factor authentication

Remote working – when employees perform their day-to-day role away from a central office for all or part of their working day – is an important benefit of the increasing sophistication of IT networks. Electronic communication has revolutionised how organisations can be structured, helping to create radical new business models for even the largest multinational corporations.

There is no longer a need for large numbers of workers to be housed together under one roof, whilst ‘virtual companies’ can appear with no physical headquarters whatsoever. The ability to access internal systems from anywhere in the world through a simple phone line or over a wireless network now means the same tasks can be completed from an employee’s home or other remote location, any time of the day or night.

In this way, organisations can capitalise on today’s 24/7 global economy and increase productivity, for example by moving key business functions offshore to lower-cost economies. What’s more, flexible working can play an important role in an organisation’s human resources policy, and the practice could well receive legislative support from the UK government in the future. There are further potential benefits in terms of business continuity and sustainability which this article will also explore.

However, remote working is not a panacea; otherwise we would now all be working from home, and office districts the world over would have become ghost towns! The flipside is that not all employees enjoy it and many miss the

structure and social interaction of an office environment. Employers too can fear a loss of control and, not least, the potential threats to data security that remote working entails.

### Losing it

The most obvious of the data security threats relates to the physical removal of sensitive data from a central secure location. Before working off-site, many employees typically take hard copies of documents with them, or download these onto laptops, discs, memory sticks or other devices, so they have all the material they need to pick up on a project again at another location (with the intention being to upload the revised material back onto the main system when they are next back in the office).

One only needs to think back to media coverage of these documents and devices being lost, stolen or left in unsecure locations to realise the enormous potential danger – and damage to reputation – associated with such actions. After the recent discovery of a memory stick containing (albeit encrypted) user names and passwords for the UK Government’s Gateway computer system in a pub car park, Prime Minister Gordon Brown went so far as to say that ministers could never guarantee the security of sensitive data.

Such a high-profile admission may suggest that nothing can be done. Of course, human beings will always make mistakes but the IT industry should be promoting effective data security to encourage the spread of beneficial business practices like remote working

further and to minimise the threats.

### A two-factor solution

One way to do this is by introducing two-factor authentication (2FA) for every occasion that a remote user logs on to access a central IT system. 2FA is a system of authentication based on something a user knows – such as a password, code or phrase – and something they possess which is hard to counterfeit and which provides additional proof of identification. In most applications, the entry of a one-time password (OTP) signifies this possession as it is generated for the user either by a physical token or during the log-in stage itself when it is then communicated to the user via a device like a mobile phone. By definition, the OTP is randomly generated and must be inputted by the user each time they log on.

In this sense, 2FA provides far greater security than traditional ‘username and password’ solutions which can be overcome much more easily and are increasingly seen as insufficient to protect data effectively. This is especially true given the sometimes obvious nature of the information used – such as real names and dates of birth – the fact that log-in details like this rarely change, and also given the tendency for users to make them easily accessible by writing them down, saving them locally, or choosing the ‘remember’ option on a software program.

2FA negates the need for any data to be physically taken away on a portable device, thereby removing the risk of loss,

### The author

Michael Robertson is founding partner and managing director of Commerce Media Limited.

### Michael Robertson

considers the business and environmental benefits offered by remote working and discusses the role of two-factor authentication in enabling this way of working.

theft or unauthorised access. Laptops and other devices can still be used by remote workers but they become merely tools to access centrally-stored data rather than methods of carrying data in their own right. If a laptop equipped with a 2FA system is stolen or lost, it will remain useless for accessing a network even if the password is easily found. Access requires the possession of something only the authorised user has and a log-on process that requires a unique, randomly-generated, single-use password.

### Mobile convenience

Moreover, in most 2FA systems this OTP is transmitted out of channel, that is, via a different medium to the one being used to access the system itself. An example would be an OTP being sent as an SMS text message to a mobile phone, enabling the user to log-on securely via a laptop or PC.

Using a mobile phone in this way has many advantages. The technology is familiar to most users and the public's reliance on their mobile phones for everyday communications means it is nearly always to hand (or quickly remembered if it is not). At times when there is no network coverage, or whenever the user so chooses, most 2FA systems are configurable to enable transmission of OTPs via other channels such as e-mail, or they can provide a series of OTPs in advance – with a given lifespan if required – so the user can log-on in any situation.

Another key advantage of this scenario is that no additional hardware or token

needs to be purchased or deployed, reducing both the cost of 2FA implementation and its environmental impact.

### Green is good

This last fact illustrates how 2FA-secured remote access can link into the green agenda that exists at the heart of business today. Both public and private sector organisations are beginning to see real value in sustainable business practices, and are being actively encouraged to reduce their environmental impact, not least by central governments trying to meet their own international obligations on carbon emissions.

One way they can do this is by offering employees the perk of working remotely, giving them more freedom with the promise of increased productivity, loyalty and morale in return. From an employer's perspective, this can also free up office space, reduce overheads and cut carbon emissions from the number of people having to commute to a central location.

### To be continued

A further benefit of operating a decentralised workforce is the measure of protection it provides if the worst was to happen at a central location. Disaster recovery and business continuity are issues increasingly being addressed by all types of organisations, but especially larger ones where the consequences can have the most impact.

In a business IT context, a 'disaster' can mean anything from the failure of central systems due to a security breach or power

outage, to severe weather, natural disaster (for example the UK floods of 2007), pandemic illness or even a terrorist attack. In any catastrophic event, there will be a need for the organisation to minimise the threat to life and continue operating with the least possible disruption. However, it is precisely at such times when data systems are most vulnerable and the need to access them greatest. Hence the motivation for ensuring that secure remote access is built into a business continuity plan.

### A remote future?

The risk of not controlling access sufficiently in the context of remote working is clear. An authorised user armed with an obvious password and no further gateways to pass through can reach right into the heart of an organisation's central IT system. It's the equivalent of leaving your house keys under the doormat.

The additional security provided by 2FA can remove the fear of unauthorised access threatening data security and provide a positive alternative to the use of portable devices for data transfer. In this way, it opens up even greater possibilities to harness the wider benefits of remote working.

With employers increasingly looking at flexible working as a means of increasing motivation and productivity, reducing overheads in the face of high energy prices, meeting environmental commitments and improving business continuity, working remotely is becoming a highly accessible proposition.