

# Don't leave remote workers to their own devices

Following the extension of legislation earlier this summer concerning flexible working regulations and an impending slew of further such directives, the ability to provide for remote working is top of the agenda for many employers. Whilst this can seem like yet more red tape for businesses to deal with, the capacity to work when transport networks are down or the gas man has promised to turn up means that remote working can be an extremely valuable tool. But while it has many benefits for both employees and employers, there are serious security and business challenges which need to be taken into account when accessing business networks, for example problems can stem from poorly secured home computers through to wi-fi hotspots in cafés and bars. For remote working to operate successfully and bring real benefits to both businesses and employees, a balance must be struck between the freedom of workers to access the network as they please, and the right of the business to secure that network in the most effective way possible. It is the finding of this balance and the best ways in which to tackle these threats which this article will attempt to address.

Being able to work remotely has massive benefits for employees and employers alike. Not only can workers make the most of what might previously have been 'dead time', such as train journeys or waiting for a flight, but it also means that workers in satellite offices or small branch offices such as regional sales reps can operate in the same way as those in the main office building, with access to all their e-mails and company networks. For employees, the ability to work away from the main office can have a positive impact on their frame of mind as they can better manage the balance between their work life and their family life. This includes the ability for example of parents to be able to work from home if a child is sick and has to miss school, but being just as effective as they would have been in the office. This flexibility allowing for remote working does not only increase employee loyalty, but is also a good recruitment tool, and businesses offering flexible working practises tend to attract a wider spectrum of employees.



However, the technology that makes all this possible has also opened the door to a number of security related challenges, and these must be addressed. Problems arise because the technology needed to work from home often includes more than just access to the internet, and according to recent research, 87% of workers<sup>1</sup> admit that they are responsible for the security of their own PCs, which they will be using to connect to their company network. In a recent report published by the House of Lords on Personal Internet Security,<sup>2</sup> it was found that one third of home computer users didn't even know if they were accessing a secure web page or not. These statistics taken together with the fact that the average cost of a UK company's worst security incident in 2006 was £12,000<sup>3</sup> should prove a serious concern for businesses, and any investment companies make in hardware and software such as firewalls to try and protect their networks from viruses, Trojans and other security breaches will be useless if just left on the shelf.

Security issues are not just limited to employees working from home. In a café, for example, what may seem like a harmless five-minute log-on to the office network through shared wi-fi might not be so. Hackers using a technique known as 'sniffing' can intercept

1. TNS Media 2007 – available on request

2. House of Lords Science and Technology Committee, Personal Internet Security report, August 2007

3. Information security breaches survey 2006, PricewaterhouseCoopers / DTI, 2006

data packets as they travel through the air stealing confidential business critical information. In addition to hackers, there is also a worrying phenomenon involving 'rogue access points,' where hackers set up their own equipment in an area already providing wi-fi access to the public, and then offer them a network connection of the same name as the one offered by the café itself. This causes confusion for users, and they may click on either network for their connection. This means there is a 50-50 chance that employees are haplessly allowing cyber-criminals access to every single confidential piece of data sent.

However, it is up to employees to demonstrate caution when connecting in public, working with business' established security encryption tools to protect data they send and receive as best as possible. While it is important that venues providing wireless hotspots take responsibility for the security of their wireless access, businesses must take action to protect themselves too. If allowing remote access to their network, companies must provide and educate on enhanced security measures to protect themselves. If they fail to do so, it is akin to leaving an office door unlocked and allowing burglars in to steal anything they wanted, with little likelihood of being traced.

While security is an issue for businesses trying to gain benefits from allowing employees to work remotely, there are also privacy issues which need to be taken into consideration. One of these is the accessibility that companies should have to personal computers. If a private computer is being used to access company files during work hours, it could be exposing the corporate network to external threats and vulnerabilities. As such, companies must be able to control the content being viewed during the business day, but a compromise may be that these controls and any monitoring be switched off outside working hours. This will prevent the IT department from filtering irrelevant sites such as those accessed by children, and will also protect the employees' privacy.

Education is also very important, and remote workers need to be educated on the best methods of securing their systems, from the effective operation of basic security software such as antivirus and firewall software and hardware in order to protect against viruses and Trojans, to more advanced security hardware.

In order to prevent any damage to a business or its network, businesses should be offering advice to

employees from their office IT service providers about what else they can do to protect their networks. For example, using a VPN (Virtual Private Network) to connecting to a company network is one of the safest methods for ease of connection and security. VPNs take many different forms, but their basic function is to use a tunnelling protocol and encryption to keep data secure as it tunnels through the internet to connect with a specific network that the user is linked to. The encryption and tunnelling means that the data being sent is kept completely separated and sealed off from the rest of the Internet, and this allows remote workers to access their office networks securely as they could if they were actually in the office. As the workers are accessing their company networks, it should be the company's responsibility to ensure this equipment is in place, and employees know how to use it. In addition to this, it should also be the IT manager's responsibility to create and deliver clear security policies and guidelines for employees to follow to avoid further risk to business networks.

Using a VPN also allows for greater protection of the network through provisioning for varying levels of authentication. This can be done in many ways, including biometric devices such as fingerprint recognition to gain access to a network, or digital tokens that provide a changing password which is synchronised with the network to allow access. Authentication does require some education in order to ensure employees are comfortable working with the security technology, but installing such hardware and providing training may be far less than any risk associated with security breaches, and the associated reputation damage and possible financial penalties.

Responsibility must be shared by all parties to ensure security of confidential data and networks as a whole. Businesses need to become wise to the poor levels of knowledge surrounding security, along with the potential damage that a virus or a data leak might cause them. With employers and employees working together to address security and privacy issues, accessing business networks remotely need not be a dangerous activity, but instead an opportunity to improve employee productivity and effective working as a whole. Hacking threats will only become more elaborate and complex as the Internet develops further, and companies need to stay ahead of the game in order to keep all their data and IT systems safe, but this can really only be done in conjunction with those who are actually accessing networks remotely.