# Just how advantageous is the *Bring Your Own Device* phenomenon?

By Sonia Blizzard

*In this article, internet security expert and MD of Beaming, Sonia Blizzard, discusses the pros and cons of BYOD and what businesses should look out for when it comes to security.*

Bring Your Own Device (BYOD) was kicked off by the smartphone and tablet revolution. As soon as everybody had their own powerful machine in their pocket workplaces deemed it useful to harness this power which we bring to work ourselves.

BYOD gives employees and employers more flexibility; It also allows people to use mobile or cloud apps to share files and folders, and well as take advantage of the functionality offered by many smartphone and tablet apps on the market.

However, while the flexibility and functionality of BYOD is certainly enjoyed by many there are some serious risks that come with it – especially when it comes to putting it on to the secured network. In fact, the phenomenon of BYOD is fast going full circle as IT departments are deeming the idea a security threat once employees take advantage of the unrestricted freedom of using mobile and cloud apps without the company having any control of how or where their data is stored, accessed and used.

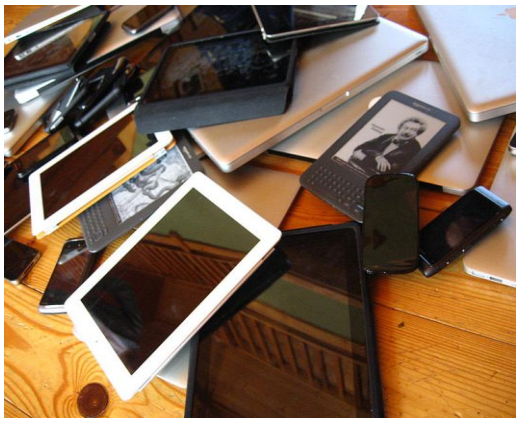
Data security is hugely overlooked by many companies and employees the world over, as many people believe that their storage is automatically secure, without checking the location where it is held or the level of authentication to access their data.

However, the problem with using employees' own devices is not just that the storage of information could become vulnerable. Other issues for companies of late have been the use of apps or links that make the phone or the tablet more vulnerable to hackers, therefore increasing the likelihood of data leakage and the loss of information about your business, your clients, your employees and other sensitive details. Certain celebrities have found this to their cost when highly personal photographs were published from their cloud storage due to this kind of vulnerability.

It's also not just the companies that have security fears over BYOD; employees are well within their rights to be concerned as well. One way of gaining the flexibility of BYOD without losing control of company data is for the company to secure these personal devices, which ultimately makes them accessible by the company.

To many employees the thought of their employer gaining access to their personal data is uncomfortable. The blurring of personal and business use raises interesting questions regarding control.

While some of these fears may be far-fetched, once a device is unsecured it is possible to do almost anything with it, and a survey recently conducted found that over 30% of people who use their own devices for work have no security features enabled on it.



And from the 70% who did have security features enabled, that security was only the four digit password that is offered with the mobile phone.

These statistics make BYOD seem like a dangerous idea, as employees are carrying around with them the latent ability to hack into a company's sensitive information just at the touch of a button. With applications such as company email, log-in information for the corporate network and proprietary data, once one of these devices falls into the wrong hands a company would have to work very hard and very fast in order to prevent harm.

BYOD is going full circle. The first time a company thought about allowing employees to use the devices that they already owned and loved for work purposes, as well as personal use, the advantages seemed tantamount for all involved. Employees' satisfaction levels increased, thanks to their more flexible working conditions, and with it their productivity. Companies were happy too. BYOD automatically brought cost savings and increased productivity meant a more efficient workforce, happy clients and profit.

However there was a downside. While it seemed like BYOD was a happy playground that we could all

enjoy, the truth is the concept is turning back around as we discover the complications and negative effects of the use of employees' own devices for business.

For companies, problems lie with control over what level of data is accessed on these devices, and the issues around forcing any kind of sanction or restriction on employees' use of their own devices. The original convenience has been replaced with complexity.

The biggest risk in rolling out BYOD is for companies to do so without having any kind of policy in place beforehand.

A BYOD policy is up to the business, but data and the device should both be secured so that you and your employees are free from all worries. One simple way of doing this is to look at having connectivity specifically set up for mobile devices, distinct from the corporate LAN, alongside a strict policy on the use of company data. It just requires careful thought. BYOD should be a convenience, flexible and hassle- free.



## About the Author

Sonia Blizzard is the Managing Director of Beaming – a company that provides secure internet connectivity and data back-up services to a number of businesses across the UK. Coming from a corporate background in the telecoms industry, Sonia worked for a firm which is now known as BT Global Services, setting up Beaming in 2004. The company bridges the gap between actual business needs and IT; specifically the broadband and telephone connectivity that's vital for running a business day to day.

## Co-ordinates

E-mail: sonia@beaming.biz
Website: www.beaming.biz
Tel: 01424 462661

## Important Notice