Make sure smartphones don't pose the biggest threat to your business security.

To secure or manage anything, you need to have some control over it. Simple, yes?

For years, IT had complete control over its domain. If you wanted a piece of software or a new phone, you had to ask IT for it. And there was a good reason. If something went wrong, IT had a better chance of fixing it quickly because it knew the environment so well. It also knew which software was installed and on which hardware because it either chose or authorised it in the first place.

But the model of IT having this exclusive control has been slowly eroded in recent years. The so-called 'consumerisation of IT' (where major technology innovations are largely fielded to consumers first before making their way into businesses) has turned IT on its head. Employees are now buying the best and most innovative technology for their personal needs and can download any piece of software they want within seconds; so they are baffled when their employer expects them to jump through hoops just to update Office 365.

The reaction to this shift in employee expectation has been the trend of Bring Your Own Device (or BYOD). In businesses with a BYOD policy, employees are not just allowed to use their own devices at work, they are actively encouraged to do so. Employees generally love BYOD because they can use the technology they want to use and don't have to carry multiple devices. Businesses love it too, because employees are more productive and they often don't have to spend as much on new hardware. But this change in ownership has eroded the control, and with it the protection, that IT once provided. With the cyber security attacks against businesses on the rise – particularly with the current epidemic in ransomware hitting businesses of all sizes – is it time for IT to take back control?

Unintended consequences

The most popular device employees want to use at work is their smartphone. The challenge here comes from their unique combination of ultra-portability, high computing power and 24/7 connectivity. At the very least, a smartphone will have access to the company's email system, but it could have access to the company's VPN and run a number of proprietary apps with direct access into the ERP system.

By their very nature of being mobile, smartphones probably pose the biggest risks to information security in an organisation. Imagine someone picking up their PC and walking out the door with it every time they leave the office. This is effectively what employees are doing with their smartphones. However, as a result of BYOD, a large proportion of these devices aren't even provided by the organisation and therefore are often not managed by the IT department.

So instead of walking out the door with their PC, it's the equivalent of bringing in their home laptop – complete with all the unapproved apps (potentially riddled with spyware, ransomware and viruses) their teenage children downloaded the night before – loading it up with corporate data and walking back out with it.

A third way: Enterprise Mobility Management

It is clear that when it comes to BYOD, organisations need to balance user freedom with the control necessary for security. A totally unmanaged device with full corporate access is a significant security risk, but most employees do not appreciate their employer taking their new iPhone 7 – which they paid for themselves – and loading it with onerous security applications and restrictive policies. It is seen as an invasion of their privacy and overstepping the line between work and personal life. The result? They simply 'go rogue' and don't tell IT about their device, undermining the organisation's security policies in an instant.

Businesses cannot turn the clock back on BYOD, so they need to find a way to manage devices that maximises security while minimising interference. The method that many businesses are turning to is Enterprise Mobility Management (EMM), which provides a single dashboard for monitoring, managing and securing an employee's mobile device. EMM allows businesses to set access controls for applications, data, apps, email and pretty much anything else within any device it is installed on. To the user's delight, EMM does not bloat their phone with visible corporate controls. In fact, EMM can partition the device to separate work and personal applications and data. This prevents the employer from gaining access to personal information and if the phone is lost and needs to be remotely wiped, only the work data is affected.

EMM is fast emerging as the next essential cyber security tool for businesses. I believe it will soon be considered as much a necessity as antivirus software, firewalls and VPN. It is essential for BYOD environments because it addresses all three areas of mobile security – the devices, the applications and the information stored on them.

The reality is you cannot undo innovation. You can only embrace and work with it. EMM is the third way for businesses, allowing them to maintain the BYOD policy that has proved so popular with employees while giving back enough control to IT to keep the business safe.

Who knew being in control could be so freeing?

Lorrin White
Managing Director

BAMBOO
CONNECT GROW