Management Briefing:

Bring your own device - Effective policies and practice

Bring Your Own Device (BYOD) is now ubiquitous amongst enterprises. For IT leaders this has meant developing and maintaining effective policies and practices to keep the organisation secure and efficient, whilst managing a proliferation of devices.

Analyst group Gartner predicts that by 2014 some 90 percent of companies will support corporate applications on personal mobile devices. By then, 80 percent of companies will have a mobile workforce that uses tablets, with the iPad expected to dominate the market through 2015, it says.

The benefits of BYOD include a richer user-experience for staff, who get to use their own, familiar mobile devices and work more flexibly in terms of time and location. They also carry with them a platform suitable for corporate social collaboration, which is 'always on', and this has benefits for team working, customer service, and closing deals, among other things.

But for the IT department, managing and securing these devices can be a significant undertaking. Peter Cox, CEO of VOIP security supplier UM Labs, says, "The security challenges facing any mobile device, not just tablets, but also smart-phones, are broader in scope than just data security issues. As the Leveson inquiry (into media ethics) is discovering, security and integrity of calls and voicemails is also an issue. These issues are the same regardless of whether users are running their own device or an official company device."

He adds that all mobile devices must be provisioned with the appropriate security controls to address data integrity, data privacy and malware, and should have a remote wiping function in case the device is lost.

Other issues that require consideration include the level of BYOD the organisation wants its IT department to support; whether it wants to block certain devices or mobile sites and apps; and the balance of mobile work to leisure usage staff are allowed during office hours.

Mobile Devices Management (MDM) technologies can help address some of these issues, and enforce BYOD policies. MDM enables IT managers to track, manage, block and enable particular devices and mobile apps, but the range of products available is very broad, with many offerings still maturing, says John Sidhu, partner at IT consultancy Glue Reply.

He says the Gartner Magic Quadrant on Mobile Devices Management shows the market is fragmented and companies should consider waiting until it matures further before buying a solution, or else choose MDM as-a-service in order to avoid costly lock-ins.

In general, Sidhu feels that BYOD works best where there is agreement between business and IT managers. "Most organisations are happy to support people bringing in devices to the business.

But it's happening out of the control of the IT department; and with senior staff doing this, it's forcing the issue. One significant insurance provider we work with had one part of the business that decided to purchase iPhones, even though it was not approved. It meant the security team had to work around their existing policies and sort out the security retrospectively. That's not ideal; it would be much better for businesses to work to an agreed framework for such deployments."

Double-edged sword

According to Martin Lunt, principal advisor at KPMG CIO Advisory, "BYOD in its many forms is a double-edge sword. On one hand, the idea that a business can leverage personal devices would seem to offer a cost reduction and, if implemented correctly, boost performance. On the other hand, agreeing to BYOD can seem like opening Pandora's Box, with a whole range of delights waiting."

Among these 'delights', says Lunt, are the need for security and compliance through authentication, encryption, records retention and discovery. IT teams may also need to provide device management and support through such things as break-fix, restore, access rights, application install, and management of software assets, patches and policies.

Corporate network access has its own best practises, relating to Wireless LAN, WAN and LAN utilisation, QoS, and network access control; and IT managers also need to ensure there is enough bandwidth to cater for the significant increase in network and bandwidth usage, due to increased demand.

Lunt adds that CIOs also need to consider the range of devices, and think about whether they require virtual images and replacement OSes and applications, in case of failure. Finally, there may be legal, contractual, tax and total cost of ownership issues associated with supporting BYOD, says Lunt.

"While the corporate benefits of implementing BYOD may not be immediately obvious, lurking under the glossy - and somewhat hyped – (Steve) Jobs vision of the future, there is definite potential for developing new working practices that can help differentiate a business and improve performance. But, for CIOs and their departments, the BYOD concept requires implementation that works for both user and organisation and that can be a complex task. Issues ranging from security to mobile contracts, device deployment, industry regulations and tax implications all have to be considered."

He concludes, "BYOD is yet to mature, so a key aspect of implementation is cross-referencing benefits and challenges with operational dynamics - data storage, appetite for risk, and so on - and configuring a workable offering."

Making BYOD work

Phil Quinn is the ICT Manager for New College Swindon and has just completed the rollout of a BYOD scheme for staff and students. He manages a network whose size and complexity would cause sleepless nights for many corporate IT professionals. Quinn currently provides IT support for around 13,000 students at the college with many of these bringing in their own device. The New College team have had to ensure compatibility with the network, and bandwidth availability for the wireless network.

Quinn says, "Our experience of BYOD dates back to many years ago, when we were simply trying to manage the sudden explosion of iPhones connecting to the campus network."

Today, approximately 1,800 of the college's 13,000 students bring in their own devices and connect to the wireless network. "It's my job to make sure it's a seamless user experience," says Quinn.

He adds, "We have a very inclusive programme at New College Swindon and don't restrict any devices coming onto the network. Whilst we've considered Mobile Device Management, for us it doesn't work. We can't say 'no' to someone's old PC or a tablet that's not as popular as others, and then say 'yes' to the more mainstream ones. Of course, this presents a number of integration challenges, but it's a question of risk versus reward."

The college has enhanced its IT system in several ways, and in particular, its wireless network. "Network coverage is key to any BYOD scheme: there's no point allowing users to bring their own device if they have poor performance whilst doing so, or can't even access the network from particular areas. You can access our wireless network anywhere on campus," comments Quinn.

"To that end we enlisted wireless specialists Xirrus to implement a high-capacity wireless network and the UK's first wireless-only annexe, to make accessing applications and education programmes as well as Internet-browsing simple," he says.

The college also increased the uplink to the Internet, replacing a 50Mb connection with a 1GB one. This gives students high-availability access to the Internet, and lecturers can use wireless devices to stream YouTube videos during tutorials. The old system was not able to cope with this level of demand.

The college is currently upgrading its firewalls to allow greater control and data throughput, and to support an increasing demand for Machine to Machine (M2M) communication throughout the campus. This M2M communication involves interactive projectors, smartboards, and other digital displays, which are connected wirelessly and can be operated remotely using PCs and mobile devices.

Quinn says, "At the start of the network revamp, I was told by some that M2M wasn't possible because of the amount of data that goes across the network. So to now have all these devices connected wirelessly and working flawlessly is incredible and making a big difference to the user experience."

Meanwhile, the college has updated its ICT policy to include mobile technology, but has ensured the same rules apply whether a campus-owned device or BYOD device is being used. "We take the approach to block and censor what is absolutely necessary, such as pornography and illegal sites, but allow the use of social media and nearly anything else."

Quinn elaborates, "We find if we drastically changed our policies to where restrictions on social networking or a number of content sites are made, then users will find a way around it. We don't want users playing with proxies just to work out how to access Facebook, as this makes monitoring the network extremely difficult."

The example of New College Swindon illustrates that it is possible to fully embrace BYOD and reap the benefits, both from the perspective of the organisation and its end users. However, to make BYOD work takes strategic thinking, IT leadership and security and compliance knowledge, as well as having the right technology and policies in place.