Computing Viewpoints

Bring your own device

October 2012
Bring your own device

Contents

Introduction ................................................................. p 3
The BYOD challenge ....................................................... p 3
Securing the mobile workforce ....................................... p 5
A growing divide .......................................................... p 6
About Intel ...................................................................... p 8
Introduction

The “bring your own device” (BYOD) trend presents a complex challenge to the enterprise in terms of standards, interoperability and security on the one hand, and personnel management on the other. In this regard, it goes right to the heart of a redefined role for IT leadership.

Today’s IT and corporate information strategists have long been told to focus more on business enablement and less on low-level maintenance. At the same time, some IT leaders are aware that corporate IT has, in general terms, slipped behind a wave of consumer technologies, which have enabled new behaviours among a broad mass of the population. BYOD is at the centre of both these issues.

“The IT marketplace is skewed in favour of consumer devices, applications and platforms”

The BYOD challenge

BYOD, in which organisations embrace and manage the usage of employee-owned devices in the workplace, is a challenge insofar as the IT department may have had zero involvement in the purchase of each device, while its owner may resent any enterprise involvement in its management. BYOD creates tension if not properly managed.

However, IT leaders – and the wider organisation – are still responsible for these devices in the broadest sense, because they may be used to access corporate applications and core data, the security of which is covered by corporate governance rules and regulations. Not supporting these devices is not an option, while turning a blind eye or issuing blanket bans on their usage during office hours risks creating major security blindspots.
IT leaders may not have had any say in the purchase of these devices – which may be laptops, tablets, smartphones, iPhones, BlackBerrys, convertibles or other devices, containing a range of different operating systems and applications – but they cannot wash their hands of any responsibility for their management and usage.

The situation is made more complex by the fact that, for the organisation, official IT purchasing is typically slow – a matter of big capital expenditure and rolling, enterprise-wide upgrades – while for the employee, the very latest devices may come free with whatever mobile contract they’ve chosen. Meanwhile, Christmas Day has become the IT leader’s nightmare, as he or she knows that the first day back to work will bring dozens of new, insecure devices into the enterprise.

In short, two procurement streams exist and they move at different speeds, skewing the IT marketplace in favour of consumer devices, applications and platforms. This creates heightened expectations for the performance and status of enterprise technology in the workplace.

For IT leaders, this can be a major headache. Employee devices may not meet organisational standards or needs. Equally, they may be insecure or compromised, unable to interface directly with corporate systems or applications, and represent a weak link in the security chain – in terms of theft or malware, for example, or locally stored login, password or IP information.

The challenge lies in deciding how far “into” the corporate IT environment the device, and its owner, should be allowed as a matter of policy, and what authentication procedures need to be adopted, both within the workplace itself and remotely in terms of VPN access.

But BYOD should also be seen as an opportunity for employee engagement and motivation, improved security policy management and, over time, reduced IT purchasing costs.

That said, BYOD should not be seen as an invitation to staff to take part in a DIY culture where anything goes, but rather as a pragmatic observation about human behaviour in a world where on-demand technologies, social platforms and peer-to-peer media sharing are the norm for most people.
IT leaders need to assert their authority in terms of how these devices are managed, in what circumstances they interface with corporate data and enterprise applications, and how employees access the organisation's systems from these devices (if at all). This means IT leaders putting themselves in the driving seat of an enterprise-wide, scenario-planned IT usage and security policy.

Indeed, looking at the challenge in that light reveals that, far from being a problem that makes IT leaders' lives needlessly complicated and frustrating, it is actually an opportunity to put themselves firmly at the boardroom table in terms of supporting the business.

Good management and clear, realistic policies that recognise the advantages of the more flexible, mobile working culture enabled by BYOD would show IT leaders in the best possible light.

All employees – and all businesses – want technology that is as fast, intuitive and available as possible. For most consumers, however, that benchmark has been set by the platforms they use outside the office. It stands to reason that many will bypass local obstacles and use whatever technologies they feel comfortable with to get the job done – and for business leaders, employees’ skills are more important than the technology platform they use.

**Securing the mobile workforce**

Accommodating user-owned devices into a fully supported, secured and managed corporate environment is the key. IT leaders need to ensure that vital data is held securely, connectivity is reliable and applications behave consistently – especially as some tablets and smartphones are vulnerable to malware, sidejacking and theft.
This itself is a challenge. IT leaders are familiar with the broad spread of security threats that affect core enterprise systems, but being faced with a mass of disparate, employee-owned devices that use different operating systems and apps means adopting a smarter, more forward-thinking security policy.

That said, it is better to accept that, in many cases, employees will use their own devices to some degree either at work – to access their own networks of contacts via social media platforms, for example – or for work out of hours. The alternative is to turn a blind eye, which is far more dangerous.

For many people, the once-clear divisions between office and home have become blurred, with many people working on corporate documents or fielding work calls and emails at home, in cafes or on the commute to and from the office. This has happened partly because of the speed at which consumer technologies and platforms have moved relative to enterprise IT, and the productivity gains should be taken seriously by the enterprise.

**A growing divide**

*Computing*’s own research findings are stark. A recent survey of more than 300 senior IT decision-makers across every sector of the UK found that, in 67 per cent of cases, more staff regularly work offsite than they did five years ago. Despite this, over half of respondents said that their organisations do not provide tablets or smartphones – the devices best suited to mobile work.

Although staff are mobile, 90 per cent of respondents said that the only devices that are allowed to access corporate applications, networks and data are those owned and secured by the company.
Bring your own device

Looked at one way, the figures suggest that organisations are doing a good job of securing the perimeter of corporate systems. Looked at another, a huge amount of productivity is either being lost by not equipping staff with the right devices – or, just as likely, work is being carried out, but on users’ own devices, invisible to corporate systems.

IT leadership, therefore, is being questioned by employees’ desire, in some cases, to improvise their own solutions so that they can be as engaged and productive as possible. IT leaders must respond by putting clear guidelines in place and ensuring that every person in the organisation is aware of them, backed by robust data security measures that are designed for the “new normal” of a more fluid, platform-agnostic technology environment.

This is sensible for a variety of reasons, some of which may not be immediately obvious: regulators and data protection watchdogs are far more likely to take punitive action against organisations that have poor data security in place than those that have clear policies and guidelines. If it can be demonstrated, for example, that everyone was aware of data security policy and it was simply down to human error that a customer’s data was compromised, then the Information Commissioner is less likely to issue a fine.

IT leaders could be forgiven for being exasperated at the conflicting demands that are being placed on them. In a sense, today’s technology environment is like a jack-knifing lorry slipping fast on the data highway. Nevertheless, not acting is not an option.

In an environment where consumer technology innovation is swift and available at low cost, many IT leaders feel that they are no longer in the driving seat of technology standards and usage – or, if they are, that they are no longer fully in control of the vehicle. For many employees, meanwhile, corporate systems can seem antiquated by comparison with their own, which can create a sense of frustration with their performance.

For IT leaders, then, there is a widening gulf between the core corporate systems that they are responsible for managing and the employees that those systems are designed to support.

IT leaders must engage with these choices and usage trends. They should begin to see BYOD as an opportunity to innovate and to refresh the business. Indeed, seeing BYOD as an opportunity can help the organisation to better map out and manage a real-world data security policy.
About Intel

Intel is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world’s computing devices. Intel’s active leadership in the development of cloud computing extends across the cloud computing ecosystem and includes technology innovation, standards leadership, and first-hand experience – combining vision (where cloud is going) with know-how (how practical cloud infrastructures are built and deployed). This cloud computing leadership can be immediately useful as you consider and implement your own cloud computing infrastructures. Intel’s current products, as well as products in development, focus on the advances you need for effective cloud computing solutions.