iOCO

CIO CONNECT

Enabling the Mobile Enterprise: Don't fight it. Feature it.

WHITEPAPER

Enabling the mobile enterprise:
Don't fight it. Feature it.

By Alex Russell

The Bring Your Own Device (BYOD) trend is changing the organisation at many levels, from the users who expect the same ease of use at the office as they have at home, to executives who are excited by – and in some cases – equally bewildered by, the opportunity BYOD brings.

BYOD will fundamentally transform IT, and while most organisations are aware of the need for a strategy, many are unsure of how or where to start. Others are struggling to manage the trend within their operations, or struggling to obtain the benefits of a truly mobile workforce. The rigid, top-down office is dying. Mobile is the future.

CONSUMERISATION OF IT

The lines between private and work devices are becoming increasingly blurred. Users today appreciate the benefits that mobile brings to their personal lives, and they want to obtain similar benefits within their working environments. This "consumerisation" of technology will force more IT change over the next 10 years than any other trend.

However, technology in a company has traditionally followed a top-down approach, where the company buys the ecosystem and introduces it to its employees.

BYOD is challenging this traditional model by shifting the power and choice from the IT department closer to the end user. As a result, IT sees BYOD as a security and compliance headache.

The CIO sits in the centre of a vortex comprising consumerisation, distributed computing, cloud services, and the need for standardisation.

Mobile devices have already become a central part of the organisational communications portfolio, and many companies are trying to follow this evolution to the logical next step: effectively managing the heterogeneity mobility brings into an IT environment in order to harness the value it can bring.

However, just as many companies are still focused on the compliance and security risks brought by BYOD rather than the potential.

The benefits of employees accessing their personal devices for work are well-documented. From cost benefits to productivity gains, BYOD makes good business sense – if you exclude the tricky management component. Mobile 1.0 happened when the BlackBerry brought e-mail to our pockets. We're at mobile 2.0, where acceptance of these devices is a done deal. Mobility is a game changer and that means a company has to discover how that will impact its culture and empower its users to be more productive, securely. There is no one size fits all. Users are different, with different needs and, as such, any BYOD solution needs to cater for different use cases.

Done right, BYOD will allow organisations to embrace consumerisation, empower employees to choose the device or devices they need and simplify IT.

BYOD done right also means developing a strategy to ensure sensitive information is protected from loss and theft, allowing a company to meet privacy and compliance standards, instead of putting it at risk because employees are creating workaround solutions. In addition, a good BYOD solution will reduce the costs and time spent on procuring devices and configuring them, working through app compatibility, and responding to a deluge of service requests. IT can actually move its focus back to more strategic imperatives.

According to Gartner, mobility is second in the top technology priorities this year for CIOs, topped only by BI and analytics.

IT wants to serve employees, do what's right for the business, and be more efficient and strategic itself. Having a BYOD solution can help achieve this. However, even when organisations understand the benefits of a sound BYOD strategy, they often struggle to move in that direction because of the IT system they have in place.

CHALLENGES

The way IT is structured today makes effective BYOD management challenging. The IT function has been squarely at the centre of managing structured systems, apps and data. People are the users and extensions of IT systems, and devices have been standardised to make it simpler for IT to support.

It is a complex set of responsibilities, and most businesses say their IT functions can get stretched. The minutia of BYOD include how to embrace both corporate and third party native mobile apps, implementing appropriate security around the apps, managing company intelligence, developing sound policies, and guiding employees on the legal implications of the mobile world and its infinite interactive opportunities. This brings in even more complexity for IT to deal with.

BYOD is also a big driver for security concerns. Information is what defines a business. It's what determines your offerings, your competitive advantage and ultimately your bottom line.

Information leakage or theft results in financial, reputational and legal risk to organisations – potentially seeing the end to the organisation's future sustainability.

You can make a case for any of the technology trends that the successful organisations of today should be following. We're currently going through a fundamental shift in technology. We're seeing a number of disruptive technologies converging on businesses at the same time.

As the trend of employees bringing mobile devices into the workplace grows, businesses of all sizes continue to see information security risks being exploited. These risks stem from both internal and external threats, including mismanagement of the device itself, external manipulation of software vulnerabilities and the deployment of poorly tested, unreliable business applications.

Organisations that are taking advantage of the flexible workspace that BYOD provides must also deal with the myriad risks associated with letting staff use personal devices and applications. Safely giving users access to company systems and data through these new delivery methods, while managing the associated risks, is the foremost challenge of the BYOD era.

Now organisations need to be guided how best to implement a BYOD strategy, ensuring they have an environment that is closely controlled and managed while employees have access to the tools they need.

iOCO recognises that enterprise mobility is no longer about the device, and the challenges that CIOs face are more around data protection and driving down risk. We understand the proliferation of devices. We believe that end users will win the battle of choice.

THE FUTURE IS HERE!

Tomorrow's IT leadership won't be at the centre of all tactical activities to the same degree as in the past. Rather, tomorrow's norms will have IT playing a critical role in governance and self-service enablement. Users will be able to access company information and apps on their terms, with the same convenience with which they consume IT in their personal lives.

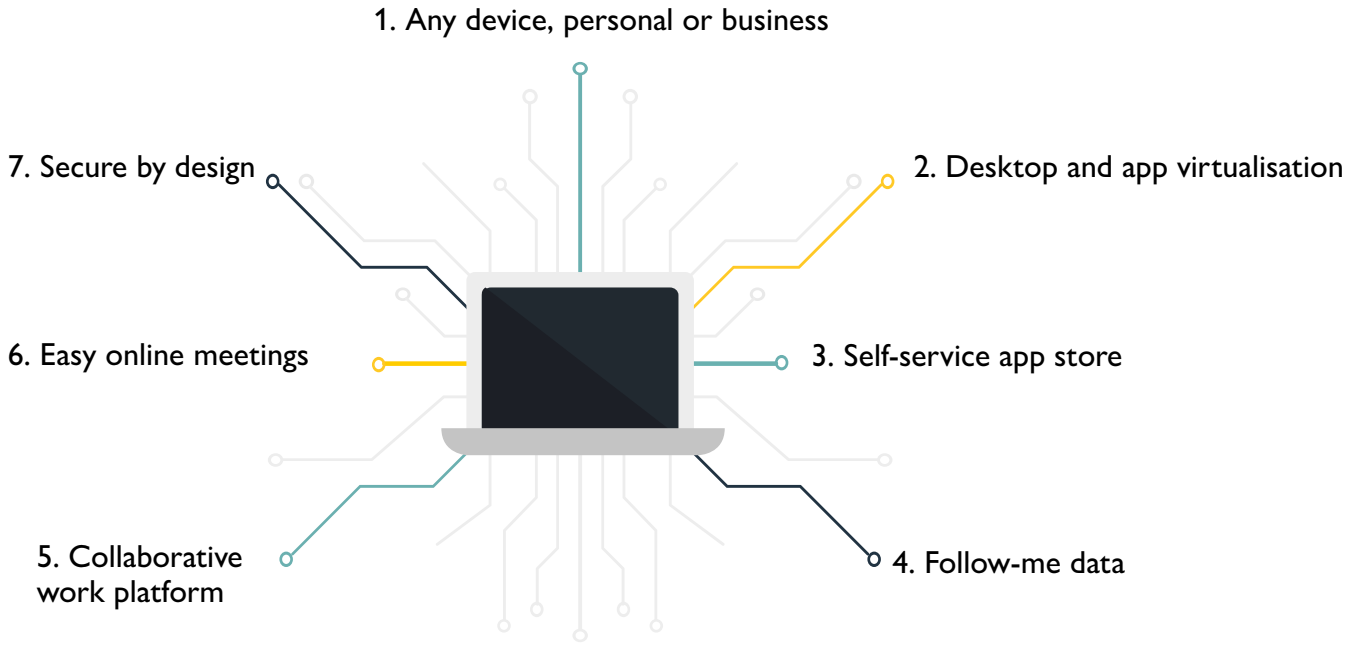
IT will be organic and unstructured, driven by tasks and relationships. Data will be created, stored, shared and accessed based on tasks and relationships, not apps or devices. Apps will be on-demand, self-service, task-specific tools.

The operating system that defines our view of a "desktop" today will be far less relevant and focused more narrowly on session management. People will use multiple devices each day without thinking about it. Devices and locations will be determined by end users. Mobile will be a dominant use case, not an occasional one.

IT wants to serve employees, do what's right for the business, and be more efficient and strategic itself. Having a BYOD solution can help achieve this. However, even when organisations understand the benefits of a sound BYOD strategy, they often struggle to move in that direction because of the IT system they have in place.

HAVING THE EDGE

There are six essential components to an effective BYOD solution:



Many companies are already moving in this direction.

THE SOLUTION:

Enterprise Mobility Management (EMM)

BYOD comes in many forms, from the ad-hoc use of personal devices to supplement corporate endpoints to replacing corporate-owned devices entirely. Whichever approach a company chooses, a complete, well architectured approach is essential for embracing BYOD without increasing risk. While not every organisation has a formal BYOD program, every organisation should develop policies regarding the use of personal devices for work.

Enterprise Mobility Management is a complete stack for managing and securing apps, data, and devices. This is a holistic approach which includes app, data and device management, providing guidance on the pros and cons, and addressing factors such as eligibility, allowed devices, service availability, roll-out, cost sharing, security and support, and maintenance.

An assessment of business priorities, users, devices, and apps, as well as infrastructure and security requirements, provides the foundation of the technology roadmap. This will allow for a well-documented design that allows the installation, configuration and building of a solution that leverages an organisation's infrastructure.

To do this, companies must evaluate the required hardware and infrastructure and what can be leveraged in terms of existing installations. In addition, the operations and support design, such as SLAs, staff required, support agreements required, etc., should be taken into consideration.

First and foremost, an effective BYOD solution must provide the ability to support any device, whether that is a personal device or a mobile device. Organisations also need a way to deliver desktops and apps to all of these devices securely.

That's where desktop and app virtualisation comes into play. When this is integrated, IT can transform any corporate application—including Windows, web and SaaS apps—as well as complete desktops – into an on-demand service available on any device. Any combination of desktop and application delivery approaches can be used to support every type of worker through a single point of control.

Any effective solution must cover scalability, performance, security, functionality, usability and interoperability.

However, this also needs to be easy for the user. As easy, if not easier, than what they have today. This is why a self-service app store is so important. For complete productivity from any device, users also need access to their data.

Follow-me data allows users to securely share files with anyone inside or outside their organisation, as well as sync files across all of their devices. In addition, IT can deploy comprehensive usage policies and remotely wipe data from devices so that confidential business information is secured, even if a device is lost or stolen, regardless of whether that device was a corporate or personal asset.

A collaborative work platform can form the heart of an organisational BYOD workspace, allowing work to get done on a social platform that companies can make their own. Not only is it important to enable a collaborative workspace, but companies still need real-time, face-to-face interaction. Simple online meetings are enabled through HD audio and video, screen sharing, data sharing, and project workspaces.

It is this approach that iOCO uniquely and effectively addresses BYOD and Enterprise Mobility.

iOCO employs a methodical, practical engagement model that addresses mobile, data and device management, coupled with a breadth and depth of industry leading security solutions

Our solution ensures that back-end systems and processes help a company embrace consumerisation. For help navigating the intricacies of the BYOD environment, talk to one of our expert consultants.

BYOD is becoming the rule, rather than the exception. Statics show that BYOD is not just a passing fad and that those businesses that don't yet have some sort of BYOD strategy in place risk lagging behind. While companies are still wrangling with the question of how to manage BYOD, users and technology are already prompting the next evolution of the trend.

ioco

Enabling the mobile enterprise:

Don't fight it. Feature it.

EOH Business Park,
Gillooly's View,
1 Osborne Lane, Bedfordview,
2007, South Africa

+27 11 607 8100
solve@ioco.tech
www.ioco.tech