Thomas Duryea LOGICALIS

Business and technology working as one

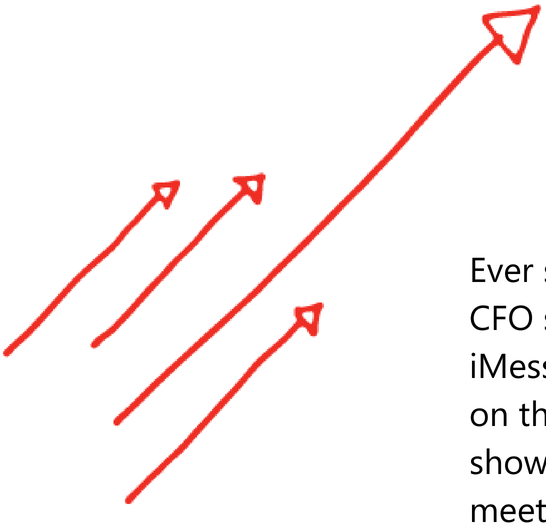
# BYOD

Why the evolution of VDI has made mobility even more mobile and how to safely incorporate consumer devices in the workplace

“As enterprise IT organisations try to meet the needs of an increasingly mobile driven business they look to a ‘Bring Your Own Device’ (BYOD) approach as a critical element of their mobility strategy. While this approach frees the IT organisation from the typically cumbersome process of certifying and procuring mobile devices, it puts the onus on IT to put in place a sustainable framework to develop the mobile applications across multiple device platforms.”

*Vishy Gopalakrishnan*
"*Work Goes Mobile*"

"The growing practice of introducing new technologies into consumer markets prior to industrial markets will be the most significant trend affecting information technology during the next 10 years." *Gartner*.



Ever since the CEO and CFO started sending iMessages to each other on their iPhones and showing up at board meetings with iPads in their briefcases instead of laptops, the IT department's hold on corporate technology and corporate data started to slip.

Sebastian Junger in his well-known book "The Perfect Storm," subsequently made into a successful film of the same name, describes a set of meteorological conditions off the USA's New England Coast that led to a storm of unprecedented ferocity.

A storm of similar proportions has been unleashed on the corporate IT function in Australia, driven by:

- A significant increase in mobile devices such as tablets and smart-phones
- The advent of downloadable Apps
- The explosion of Social Media as the preferred method of communication for hundreds of millions of people around the world
- The trend towards cloud computing.

The result is the potential for significant increases in agility and productivity - and also a very different environment for Corporate IT to manage.

The concept of Bring your Own Device or "BYOD" perhaps best represents the combination of consumerisation and pressure from employees to work in a more flexible manner.

## Workshifting

Employees today in many industries are demanding greater flexibility in where and when they work, and "work" is being increasingly defined by something you do and not something you travel to. This is witnessed by:

Qantas CIO Paul Jones in an interview with the Australian newspaper in September 2011, said he recognised IT departments could no longer dictate what employees should and should not use at work. "The old 'I'm going to control everybody's end-point device' is gone. You have to embrace it and manage it rather than try and draw really hard walls around it."

- The emergence of the virtual workspace, or "workshifting" brought on by the breakdown of the traditional office space and the 9 to 5 work-day
- The desire of users to be connected 24x7 from any location
- The expectations of the digitally savvy workforce to be connected to their digital personal life at all times.

The Citrix Global Workshifting index compiled from research completed in October 2011 of 1100 IT professionals across 11 countries (including Australia) found that by 2013, 93% of organisations will have implemented workshifting policies, up from 37% in 2011.

## Consumerisation

Corporate IT has been dealing with wave after wave of new technology for many years. What's new about this particular trend is that the technology is showing up first and foremost in consumer markets and then being taken into the corporate environment, often to the significant alarm of the IT department who are used to deploying the devices officially tested and approved by the organisation.

Users have a strong desire to access their information from any device, anytime, anywhere and if IT won't supply that access they will do it themselves.

The era of PC dominance in the corporate environment is declining and we are seeing the emergence of a new paradigm, the rise of the End Point (EP) device. Tellingly, in 2012 analysts expect that more than 50% of computing devices will be smart-phones and tablets rather than PCs.

According to a 2011 IDC study, 41% of the devices used by information workers to access business applications are ones they own themselves, including home PCs, smart-phones and tablets. That was up 10% in a single year. Interestingly, the same survey found that 70% of employees reported they already accessed corporate data with their own devices.

# Challenges

"If you don't work with users on the devices they want, they are going to do it anyway, and that's worse."
*Jim Dossias, Logicalis US*

"The challenge seems two-fold: immediately, IT must determine how to provide secure access to enterprise resources - this is distinctly non-trivial. Longer term, the mediocre user experience of the typical enterprise app must be improved if one is to translate the gains of consumerisation to business value."
*Thomson Reuters, Mobile Technology Director Dan Bennett*

Clearly, BYOD has a simple appeal for the end user: "I get to use my new smartphone or tablet at work!" What goes through the mind of the typical IT person is much more complex.

So what challenges does the IT manager face with the rise of BYOD?

- Do I have the network infrastructure to support all those access points and IP addresses?
- Do I have appropriate security in place? Actually, what is "appropriate" security?
- Do I have the necessary capability from a server perspective?
- What's going to happen to my Internet pipe when everyone who comes into the building wants wireless access?  Do I have enough bandwidth?
- What happens at the next technology or OS upgrade cycle? I now have 3x the machines to upgrade and ensure compatibility and compliance and the devices don't even belong to the organisation!

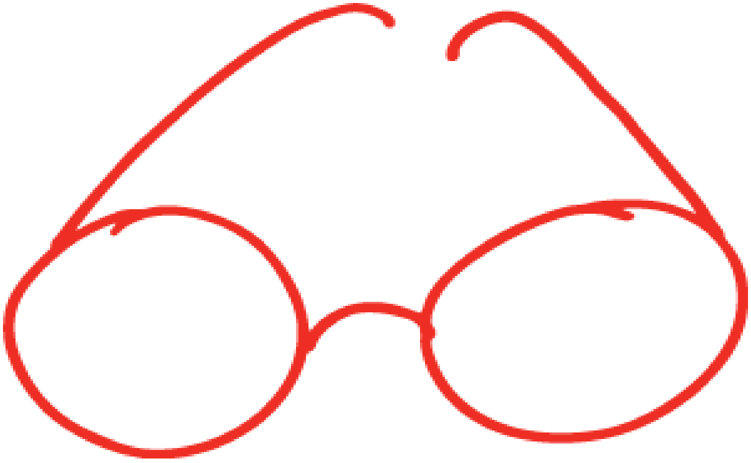
But this apparent nightmare for IT might not be so bad.

IT departments that are taking steps to enable user-owned smart-phones and tablets are cautiously optimistic. The wide area networks (WANs) appear to be able to handle the extra demand, corporate data is still secure, and all those end users wandering around armed with their own technology aren't calling them for support or otherwise bringing the whole IT environment crashing down around them.

## Beyond the IT Department

BYOD is not just an IT issue. The implications and the liabilities extend to the major stakeholders throughout the organisation including finance, legal, HR and the business' leaders.

- Consider how HR policies and contracts will need to be modified to cope with BYOD devices.
- How will this vary for contractors versus full time workers?
- HR and potentially Legal will need to be involved in clarifying what belongs to the organisation and what belongs to the individual.
- How does the company protect itself from the negligence of workers who release sensitive customer data? In some sectors protecting customer data and records is a legal requirement.
- When a device is lost and data needs to be wiped, does the organisation have the right to wipe the employees personal information?
- How do policies around inappropriate and offensive material apply when the device is owned by the employee but is used for work tasks?
- What expenses for devices bought to the workplace by staff members is acceptable to the organisation? Will the organisation pay for the voice and data plans? If so which plans are acceptable and which are not? How do organisations police what data or calls are personal vs. work without creating a huge overhead. Have the FBT implications been considered for cash payments towards employee-owned devices?
- What guidelines and training will be provided for managers to ensure staff are using devices appropriately and productively.



The table below identifies the set of considerations that need to be addressed for specific tactical and strategic IT functions.

| Tactical/Strategic Area | Considerations |
|---|---|
| **Business continuity planning and disaster recovery** | • Should non-corporate devices be granted access or restricted from business continuity planning?<br>• Should there be an ability to remotely wipe any end device accessing the network if it is lost or stolen? |
| **Host management (patching)** | • Will non-corporate devices be permitted to join existing corporate host-management streams? |
| **Client configuration management and device security validation** | • How will device compliance to security protocols be validated and kept up-to-date? |
| **Remote-access strategies** | • Who should be entitled to what services and platforms on which devices?<br>• Should a contractor be given the same entitlement to end devices, applications, and data? |
| **Software licensing** | • Should policy change to permit installation of corporate licensed software on non-corporate devices?<br>• Do existing software agreements account for users accessing the same software application through multiple devices? |
| **Encryption requirements** | • Should non-corporate devices comply with existing disk encryption requirements? |
| **Authentication and authorisation** | • Will non-corporate devices be expected or permitted to join existing Microsoft Active Directory models? |
| **Regulatory compliance management** | • What will organisational policy be on the use of non-corporate devices in high-compliance or high-risk scenarios? |
| **Incident management and investigations** | • How will corporate IT security and privacy manage incidents and investigations with non-corporate-owned devices? |
| **Application interoperability** | • How will the organisation handle application interoperability testing with non-corporate devices? |
| **Asset management** | • Does the organisation need to change how it identifies the devices it owns to also identify what it does not own? |
| **Support** | • What will the policy be to support non-business owned devices? |

# Benefits

"I spent $10 million making my purchasing system usable on SAP. I spent $10,000 making it usable on my iPhone. You do the math."
*Todd Pierce, CIO, Genentech*

The evidence is quickly mounting that the next wave of business growth and opportunity will come directly from an organisation's ability to embrace these new technologies.

Some of the benefits IT departments are reporting from BYOD involve hard savings as organisations shift at least some of the cost of the device to the user.

Additionally, The Citrix Global Workshifting index research respondents identified that cost savings are among the main drivers for workshifting.

Many of the benefits are harder to measure, for example:

- **Increased collaboration** between employees, partners and customers. The reason that smart-phones and tablets became so popular in the first place is because they do make communication easier and more natural.
- **Employee job satisfaction and retention** increases significantly when employees are allowed to flex-work or telework. It allows organisations to tap into a broader labour pool by facilitating collaboration with part time workers, contractors, outsourcing partners and consultants.
- **Business Continuity** during disruptions to the typical workday. Public transport disputes, extreme weather events, plane cancellations, attending to sick children are all typical examples.
- **Employee productivity** – Workshifting allows employees to spend more time getting things done. Access to corporate data whilst on the move or out of office hours allows staff members to continue to be productive and creative on a much wider variety of tasks, whilst unwired from the corporate network at a time and a place that suits the staff member.

## BYOD Cost Savings are a key driver

- **45%**
  **Reduction in HR related costs**
- **39%**
  **Ability to recruit labour in low cost areas**
- **38%**
  **Reduction in real estate costs**
- **26%**
  **Contribution to environmental sustainability**

# Getting There:
# The journey to BYOD

"The lightning-fast speed of adoption of the iPad into the business world caught everyone by surprise. Now business execs are showing up with their own iPads, bought with their own money, expecting full and seamless connectivity and integration between personal and business applications. It's what every CIO dreamed of, but we all thought we would have more time to prepare for these customer expectations."

Desktop virtualisation is emerging as a key technology for creating a more flexible workplace.

The Citrix Global Workshifting index found that 91% of organisations are planning to implement desktop virtualisation by the end of 2013. Of those, 57% indicated they are implementing it to enable workshifting. Desktop virtualisation enables organisations to access full desktops, applications and data from wherever they are, whenever and from any device a worker chooses. In addition, the security benefits of desktop virtualisation ensure that confidential business information is protected from loss and theft in order to meet privacy and compliance standards. People can also take advantage of online meetings and file-sharing services which allow teams to collaborate effectively, regardless of the location of every individual.

"It's not usually the role of the CEO to get directly involved in specific technology device decisions but Apple's iPad is an exception. It's more than just the latest consumer gadget and CEOs and business leaders should initiate a dialogue with their CIOs about it if they have not already done so. "
*Stephen Prentice, Gartner Fellow and Vice President.*

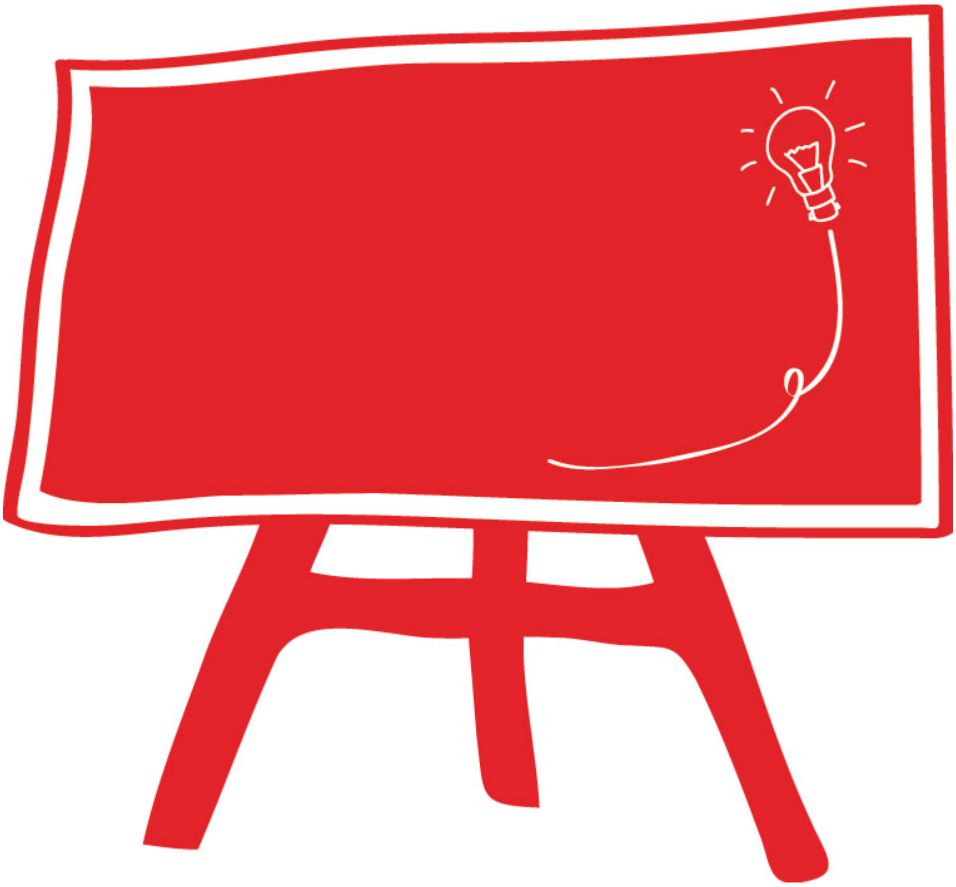
## Easing into BYOD

There are several ways to ease into BYOD. You can begin with proxy-based access to enable mobile mailboxes and ramp up to allowing trusted devices that meet a security baseline.

Enabling BYOD for specific sets of users makes it easier to monitor and manage their activity. They effectively become a proof of concept test case that you can use to evaluate your ability to enable other sets of users. And, if there's a problem, it's also easier to contain.

Deciding who owns what can be problematic. Typically, users retain ownership of their devices, but the organisation retains ownership of all the corporate data. As straightforward and reasonable as that sounds, the opportunity for conflict abounds. For example: Owning corporate data means that the IT department would have the right and the means to wipe an employee's misplaced smart-phone to protect corporate data. But what if the only way to erase corporate data is by erasing an employee's music and the photos of the kids in the process?

That's a harder call to make. A new category of mobile device management (MDM) tools is rapidly evolving to help organisations separate personal data from corporate data. But, for all the new tools that are available, coping with the rate of change that BYOD has let loose on the IT department can still be daunting.



There are so many "dimensions within dimensions" that there are lots of ways things can go wrong. IT has to crawl before it walks. We recommend a phased approach: don't roll out BYOD all at once.

## 1. Prepare Your Network

Assess and potentially upgrade your wireless network to ensure it's capable of supporting the additional bandwidth requirements of employee-owned mobile devices, including adequate Quality of Service (QoS) controls for handling of critical traffic as well as voice and video.

## 2. Implement Security Architecture and Policies

Review your IT security policy to address non-company owned mobile assets, to include:

- Definition of the allowed types of devices and operating systems
- Device and application ownership and management
- Data loss prevention and compliance considerations
- Develop a granular network access strategy to address mobile devices, including:
  - Assignment of privileges based on user, device, location and time of day.
  - Implementation of identity management and network admission control technologies that deliver device profiling, posture, assessment and/or remediation.
  - Implementation of technologies for centralised authentication, authorisation and accounting.
  - Use of content filtering technologies to enforce data loss prevention, threat prevention, acceptable use policies and general access.

> "In today's environment—in the Age of Immediacy—the CIO can't afford to be seen as a naysayer. If you don't find a way to work with the business, the business just might find a way to work without you. At many companies, you will hear stories of business units that went ahead and purchased technology after losing patience with the IT department."
> *Hunter Muller,*
> *"The Transformational CIO"*

## 3. Engage the non-IT stakeholders

Rolling out a BYOD solution by its very nature involves a wide variety of individuals and stakeholders. As with most change programmes there is ample opportunity for failure if planning is not done properly. Some areas to consider include:

- Define the "classes" of users, what BYOD policy will apply to them and how the technology will support this.
- Develop and clearly articulate the BYOD policy, including the employee's responsibility, data access permissions and who will pay for what.
- Ensure that HR and the legal department are fully engaged before the introduction of BYOD as the legal and employment ramifications are not to be underestimated.
- Communicate to employees what is supported in a BYOD environment: "The Service Desk and support staff should have clear cut criteria to determine what is supported by IT, what is supported by a third party and what is the responsibility of the employee in relation to BYOD" (Macanta Consulting).

## 4. Monitor and Manage Activity

Management of mobile devices is increasingly challenging, but organisations can transfer management responsibilities to a third party. "There is a trend toward managed mobility" states Claudio Castelli, Senior Analyst at Ovum Research. "Enterprises should look for providers that can offer device management capability and support for an increasing diversity of devices and the speed of development and new product launches in the device market."

Some of the things to consider are:

- Implement a mobile device management (MDM) strategy that can provide complete provisioning, configuration, monitoring, and reporting for connecting BYOD mobile devices.
- Implement centralised and comprehensive wireless management and monitoring tools that provide converged user access and identity management with complete visibility into endpoint connectivity regardless of device, network or location.

## Allow for the Unexpected

Following the above best practices can give an IT department the confidence to turn and face the BYOD wave. However, when you are mapping out all the considerations that need policies – and questions that need answers – leave a large territory open for the unexpected. Surprises are going to happen. This is where the ability to closely monitor and manage all activity is critical. If you can't anticipate the unexpected, at least you can see it when it happens and take appropriate action quickly.

As scary as the invasion of smartphones into your data center may be for IT, a scarier thought is the world of shadow IT that enterprising users have found outside the protective firewall that surrounds your data center. Once users have access to their own technology, if IT doesn't keep up with their requests for a specific functionality, they can find tools on Google outside of the IT department's control that will. In fact, they probably already have. While many IT departments are reserving judgment on the "cloud," end users are all over it.

## Thomas Duryea Logicalis can help you build a Roadmap to Tomorrow's (Virtual) Workspace

❶ **Develop the Business Case.** Combining an ROI and/or TCO analysis of your current environment, we help you to quantify the benefits of moving to a BYOD model and implementing a virtual workspace solution.

❷ **Engage key stakeholders.** Working with your IT organisation, we interview key staff across all business units to understand user concerns and expectations. This enables us to identify different user types within your organisation and establish different BYOD profiles for those users.

❸ **Infrastructure readiness.** We use a combination of technical tools and processes to analyse network and data centre performance, and the ability of the current infrastructure to support a virtual desktop strategy.

❹ **Build a Proof of Concept.** This final step brings the previous three steps together, using the information gathered to deploy a trial of the proposed virtual workspace solution to a selected group of users.

Thomas Duryea Logicalis is changing how organisations design, build, pay for and manage IT solutions. Recently named by Cisco as “Virtualisation of the Year” Partner in ANZ, Thomas Duryea Logicalis is highly skilled at delivering technology. We work with customers in all major industry sectors and public services to improve the experience of both front-line workers and back-office IT professionals.

**marketing@tdlogicalis.com.au**

Thomas Duryea
LOGICALIS
Business and technology working as one