A 4-Letter Acronym Sending CIOs Running Scared - BYOD

What This Means for the other 4-Letter Acronym - ITSM

Karen Ferris

ABSTRACT

Bring Your Own Device (BYOD) or Bring Your Own Computing (BYOC) is being embraced by some organisations and making others break out in a cold sweat. BYOD is here now and is not going to go away – in fact it is already happening - and therefore organisations need to prepare for, and manage the situation. This paper discusses what this means for IT Service Management (ITSM).

BYOD on the Rise

Bring Your Own Device (BYOD) is a trend on the rise and is not going to go away. Organisations have to face up to the fact that employees want to use and will use their own devices in the workplace. They are already doing it and have been doing it for some time.

Forward thinking organisations are embracing BYOD as a way of attracting and retaining talent. Students leaving school and university where they have been able to plug in their own devices – smartphone, tablet, laptop etc. – are not going to be satisfied when told by a potential employer that they have to use equipment provided by the employer and are not allowed to connect their own devices. This will be seen as archaic, restrictive and unsatisfactory. The likelihood is that the equipment being provided by the employer is inferior to the leading edge technology owned by the employee.

> On 26/07/11, Citrix Systems announced the results of the Citrix Bring-Your-Own (BYO) Index revealing that 92 percent of IT organizations are aware that employees are using their own devices in the workplace and 94 percent intend to have a formal BYO policy in place by mid-2013, up from 44 percent today. The research found that attracting and retaining the highest quality talent, increased worker productivity and mobility and greater employee satisfaction, as well as reducing IT costs, are the primary drivers of BYO adoption.
>
> "There are two reasons that BYO is being embraced within organizations," stated Mick Hollison, vice president, Desktop Marketing & Strategy, for Citrix. "There are those that are using BYO to keep up with the rapid consumerization of enterprise IT and then there are forward-thinking CIOs who have embraced BYO as a way to attract the best talent, encourage a flexible working environment and raise productivity levels."[1]

The biggest fear of CIOs is security including access to sensitive information and the chance of that information leaving the organisation. Neither of these should be new concerns raised by BYOD. Employees have had access to sensitive information for decades and the availability of CDs, USBs, email forwarding, phone cameras, photocopiers, pen and paper etc., has allowed this information to leave the organisation.

So it is time to calm down and embrace the future.

In April 2011, iPass issued the Global Mobile Workforce Report[2]. iPass surveyed more than 3700 employees at 1100 organisations worldwide. The survey found that only 27% or workers with tablets received them from their organisation. 73% were using their own tablets for work-related purposes. 94% of workers have a smartphone and the smartphone and tablet users are doing more than just email.

The top five business applications beyond email are:

- Note taking applications (47%)
- Contract or contact management (39%)
- Office suites (33%)

---

[1] http://www.citrixaccessessentials.com/English/ne/news/news.asp?newsID=2314341

[2] http://www3.ipass.com/wp-content/uploads/2011/05/iPass_MWR_Q2_2011.pdf

- Social media for work (30%)
- Web conferencing (25%)

I do not intend to discuss in detail how organisations can overcome the security concerns that BYOD poses. There is a myriad of information already available that covers that. It is suffice to say that virtualisation, security control such as "wipe and lock", GPS tracking and fencing, anti-malware and firewalls, device encryption, device fingerprinting solutions etc., and a good BYOD policy should resolve any issues.

I also recommend that reference be made to organisations such as Suncorp Metway, Citrix Systems, and Curtin University, who have embraced a BYOD approach.

Having established that BYOD is the here and now as well as the future, I want to discuss what this means for IT Service Management (ITSM).

The following are some of the key areas of ITSM that I believe have a part to play in the BYOD environment. They are not in any particular order nor do they imply that BYOD is not subject to the entire ITSM service lifecycle. BYOD should be treated like any other service but it does have some distinctive considerations.

Service Strategy

Service Strategy needs to consider the adoption of BYOD in the organisation. It may not be appropriate to every organisation and it may not be appropriate to every employee within the organisation.

Careful consideration needs to be given to the ramifications of a BYOD strategy including legal, financial, HR and the need to maintain productivity and meet service level agreements. The Service Portfolio approach of "define, analyse, approve and

charter" needs to be applied to BYOD as it does to any other service under consideration as a potential service offering by the organisation.

Demand Management needs to understand the demand for BYOD within the organisation and Financial Management needs to understand the financial impact of adoption (see below).

Once the decision to adopt a BYOD strategy has been made, this will drive corporate policies and procedures in relation to use of personal devices which will also vary from country to country due to differences in privacy laws, taxation, working practices etc.

Financial Management

Investigation into the cost of a BYOD approach including Return on Investment (ROI) and Return on Value (ROV) needs to take place. Whilst organisations may realise cost savings through reduced hardware purchases and support costs there may be increased costs in additional security and administrative systems and infrastructure investment.

Organisations may have to provide equipment allowances such as employee interest-free loans for new computers, stipends, etc. and allowances for applications purchased for work-related purposes. These additional costs need to be weighed up against the inherent purchase and support cost savings of BYOD along with the ROV of employee -engagement, -satisfaction, -productivity and -retention.

Policy

As mentioned above the adoption of a BYOD strategy will drive the establishment of corporate policies and procedures.

Gartner recommends that these policies include, at the very minimum[3]:

- Language to explain the employee's responsibility to have a suitable machine available for company use at all times
- Minimum specifications for hardware and OS
- Who will pay — and how much — for hardware, software and third-party support
- What is and isn't supported by IT organisation
- Remote-access policies security policies
- Levels of permissible data access
- Safe storage of company data
- What to do if the system is lost or stolen
- What to do at termination of employment
- Financial liabilities of enterprise and user
- Data cleansing from notebook hard drive

In addition to the security considerations that were listed earlier, the Information Security Management (ISM) policy needs to clearly state what happens if an employee loses a mobile device or leaves the organisation. For example, the

3 https://www.citrixmarketingconcierge.com/FileExplorer/Partners/XenDesktop/BYO/Gartner_Report_BYO_checklist.pdf

organisation may retain the right to wipe any mobile device of corporate data or all data in given circumstances.

In conjunction with Access Management, ISM may generate one-off, time-limited access codes. ISM also needs to prescribe what is expected of the employee in regards to their mobile devices. For example, employees may be expected to have a certain level of anti-virus protection installed onto any device they bring into the organisation.

The organisation may decree a minimum specification for employee-owned devices including a specified warranty period from the device supplier / manufacturer.

According to Lia Tim writing in IT News[4], the following is a quick checklist in relation to security for BYO devices:

- Apply to BYO computers the same security settings as an outsider connecting to the network.
- Only allow BYO computers onto the network after administrators have cleared the machine for use.
- Consider use of virtualisation to lock down a virtual machine for work use.
- Ban the storage of corporate data on the device and offer secured cloud services as an alternative.
- Ban jailbroken devices.
- Insist on encryption.
- Lock sensitive documents to devices and/or time-limits.

Service Design Package

As mentioned earlier, the provision of BYOD as a service should be no different to that of any other service and should be subject to the same service design considerations. Some of the considerations specific to BYOD are mentioned throughout this article.

A Service Design Package (SDP) should be created with particular emphasis on the security implications of the service, the technology standards associated with the service, service dynamics, support requirements and service level requirements. It is not the intent of this article to list all the aspects of the SDP in detail, but suffice to say that it should cover at a minimum:

- Requirements: Business requirements; how and where the service is to be used; contact details;
- Service Design: Functional requirements; service level requirements; operational management requirements; service design requirements; expected outcomes and deliverables including financial outcomes;
- Organisational readiness assessment; and
- Lifecycle plan: overall service programme; service transition plan (including all testing requirements); operational acceptance plan with acceptance criteria.

Service design requirements should include a service model that describes the structure of the service – i.e. how all the various components fit together and interact. This is where consideration will have to be given to which devices are to be supported for which business services as not all devices will be applicable for all business services e.g. smartphone may be used for some business services and not

[4] http://www.itnews.com.au/Tools/Print.aspx?CIID=256857

other others; tablets may be used for some business services and not others etc. The service dynamics need to be captured and may form part of the Configuration Management System (CMS).

Service Catalogue Management

BYOD should be included as a "service" in the Service Catalogue. The Service Catalogue should describe the BYOD service including (but not limited to) the following:

- what the BYOD service entails;
- standard service details and options;
- any exclusions pertaining to the service;
- who is entitled to the service (if the service view is not limited to those entitled to receive it);
- the level of authorisation and approval required in order for the service to be granted;
- the obligations of the employee (including linkage to the associated policies);
- costs such as support costs that may have to be incurred by the employee); reimbursements available such as an allowance for using a personal device and purchase of applications for work-related purposes;
- information to assist employees in making an informed decision of whether to opt-in to the service e.g. pros and cons;
- how to obtain the service;
- service level targets associated with the initial service provision and ongoing support;
- hours of provision and hours of support; and
- contact details for more information regarding the service (including avenue for complaints and compliments).

Service Level Management

Service Level Management will have to consider the service level targets for the various device types that the BYOD environment encompasses, both for initial connectivity to the network as well as ongoing support and maintenance. The obligations of both the employee and the organisation should be specified in the Service Level Agreement (SLA). For example, initial support for connectivity issues will only be provided by the organisation if the employee has accepted the conditions of service that include stated security protection on the device and three year manufacturer warranty for the device. If the organisation provides no additional support for BYOD other than initial connectivity, this should be clearly specified. See "Service and Support" below.

The SLA should clearly reflect the BYOD policy, levels and conditions of support, costs etc. either by links to the relevant information or specifically within the agreement (avoiding repetition of detail).

Release and Deployment Management

A phased approach to deployment would be recommended in order to test, validate and evaluate the outcome of allowing each type of device access to the organisation's network.

Once network connectivity is established, testing will need to incorporate the use of each device type to access each business service to which connectivity is being permitted.

Testing should incorporate as many security scenarios as possible to provide assurance that the biggest concern for this service has been given appropriate focus. As with any security breach, it is not just the potential cost of the incident that is of concern but also the reputation of the organisation that is at stake.

Change Management

If your employee onboarding is managed via the Change Management process, ensure that there is a child Request for Change (RFC) that drives the acceptance of a BYOD policy by each employee. This should provide a check that the employee has read and signed the BYOD policy before IT is allowed to grant access to that person.

This should also apply to employees as they opt-in to the BYOD scheme. The Configuration Item (CI) relating to the employee should indicate that they are a BYOD subscriber. See SACM below.

Service Asset and Configuration Management (SACM)

If you are recording employees as Configuration Items (CIs), include an attribute that indicates whether they are users of organisation owned computing (and if so what items) or using their own computing. This will allow reporting on the percentage of employees adopting BYOD over time. The trend analysis will allow forecasting to take place on predicted uptake and therefore provide insight into how much computing equipment the organisation will have (or not have) to provide in the future. This feeds into Capacity Management and the management of spare computing resource in the event of failure of employee owned equipment.

It will also be necessary for a check to be made on current software licences to ensure that the organisation is allowed to grant employees access to any licensed software that they will need to use when using personal computing devices over the network.

Capacity Management and Demand Management

Research should take place to try and predict the uptake of BYOD within the organisation. This is going to vary from organisation to organisation. Factors that will influence the uptake include the age demographic within the organisation (e.g. Gen Y are more likely to adopt BYOD than the Baby Boomers) and the nature of the work undertaken by employees (e.g. those using IT intermittently are less likely to adopt BYOD than those using it for the majority of their work).

The degree of employee mobility may also have an influence where a highly mobile workforce may be more suited to a BYOD approach than a static one where the fixed desktop is more than adequate for most employee needs.

The level of employee computer literacy within the organisation will also have an influencing factor. A highly computer literate workforce is more likely to embrace a BYOD approach as they will be more confident in the management and

maintenance and connectivity of their own devices including provision of initial fault investigation and diagnosis.

When planning the introduction of BYOD all these factors need to be taken into consideration to determine the capacity levels of computing devices that the organisation will need to provide for both normal operation and backup in the event that the employees equipment fails to work. The BYOD policy should state that in the event that the employee cannot conduct their expected duties with their own equipment that they will be provided with organisation-owned equipment until the time that their own equipment can be used. Not being able to connect your own equipment to the organisations network is not an excuse not to work!

Therefore the organisation needs to predict demand and ensure sufficient capacity of computing capability for normal and contingency situations.

There also has to be consideration of balancing demand for a BYOD approach with the complexity for the Service Desk and support teams in supporting many varied and unfamiliar devices. See below.

Service Desk and Support

There needs to be clear communication from the Service Desk to employees in regards to what is supported in a BYOD environment. This should defined in the BYOD policy.

Liz Tay writing in IT News[5] outlined the combination of tactics that organisations are adopting in regards to the support of BYOD according to the Gartner analysts.

These included:

- timeboxed support, where support staff committed a maximum of 30 or 60 minutes to supporting any BYO devices;
- "best effort" support, where support staff made "reasonable attempts" to fix problems, with the understanding that BYO problems were ultimately the user's responsibility;
- technically bounded support, where corporate IT supported some technologies and not others;
- loan device pools, from which users could temporarily replace lost or broken devices;
- community support, so employees could share information and experiences through mailing lists, corporate social networks, wikis, or microblogging tools;
- defining or providing support arrangements with third-party providers;
- outsourcing support completely to an external organisation;
- education and training programs to make users aware of common problems and solutions, BYO policies and their responsibilities; and
- policy administration and enforcement, including wiping devices or deauthorising users when necessary.

It was also suggested in the article that support staff should be prepared to provide training, education and policy auditing to prepare for situations in which a personal device may be required for e-discovery as a result of litigation.

[5] http://www.itnews.com.au/News/265821,byo-computing-needs-contingency-plan-gartner.aspx

The key is for the boundaries to be clearly stated and understood. Communicate the level of support and maintenance that will be provided to employees who bring their own devices and what minimum standards are to be met before an employee is allowed to connect their device to the network.

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.

Ensure that employees understand the level of access the organisation has to the employee's personal devices and the content held on it. This has to be defined in conjunction with HR and incorporated into policy. For example, is the organisation enabled to investigate breaches of codes of conduct on an employee's device e.g. the presence of pornography on a device used for work purposes? If a device is lost or a security breach detected, can the organisation wipe all the data on the device or will the wipe exclude "personal" data?

As with any support requirement, the Service Desk and support team should be equipped with enabling knowledge and tools.

Supplier Management

In regards to support, the organisation may wish to consider third party support for the employees participating in the BYOD scheme.

In the paper, "Checklist for an Employee-Owned Notebook or PC Program", [6] Gartner provides some advice on the third party support and maintenance considerations.

One of the great benefits of an employee-owned PC program is relieving IT support staff from dealing with PC break/fix and nonstandard software application issues.

However, one of the primary tenets of the program is the employee's responsibility to have a suitable machine available for company use at all times. If that system breaks, then the employee will need to get the support from somewhere. Requiring a hardware maintenance contract is not enough, since there will always be "how to" questions, as well as inquiries about OS and software problems. While many younger workers who grew up with PCs, as well as many technically astute workers, are self-sufficient, a significant percentage of knowledge workers will still require an organized, predictable form of support.

A best practice is to organize suitable third-party support options for the plan's participants. The support can be provided by value- added resellers, dedicated support organizations or PC hardware OEMs. In addition to hardware, the support plan has to cover OSs and application software, as well as home networking and printer issues.

Potential options are that:

- *During the plan pilot and in early stages, the enterprise can choose to pay part or all the support expense as an employee benefit. Employees can, of course,*

6 https://www.citrixmarketingconcierge.com/FileExplorer/Partners/XenDesktop/BYO/Gartner_Report_BYO_checklist.pdf

opt out.

- *Enterprises can also choose to provide "loaner" systems loaded with the corporate image. This strategy serves to keep users productive during a personal system repair period.*

Note that there is a separate, in-house concierge-level support program for executives who require faster and more-personalized service. To ensure adequate funding, executives should be charged for the concierge service.

Supplier Management should investigate the various support options available to the organisation for the BYOD environment and choose the most suitable for the requirements of the organisation.

Knowledge Management

In an environment where support for many varied devices is required (to some degree or other), Knowledge Management will be key. At a minimum, support will be required for connectivity to the network and therefore the knowledge base should include instructions on how to connect a particular device to the network.

The knowledge base should also include details of the BYOD policy and the requirements of the employee as discussed in this article e.g. minimum specification for devices, mandatory warranty periods etc.

As new device types enter the workplace, the knowledge base should be updated with the connectivity details for that device.

Collaboration tools also allow employees access to the knowledge and experience of other employees so a degree of self-help can be undertaken where employees are experiencing difficulties. Good collaboration tools and a comprehensive, up-to-date and accurate knowledge base can drastically reduce the demand on the Service Desk and support teams in BYOD environment.

Summary

As organisations start to embrace BYOD, ITSM also has to step up to the new challenges that this brings, not only in terms of security but also support.

Treat BYOD as you would with any other service and subject it to the aspects of service strategy, and service design that it warrants.

The key is to clearly define the policies around BYOD and ensure that it is communicated across the organisation in a language that can be understood by all employees. Make sure that the requirements of employees are clearly laid out and the responsibilities of the organisation in relation to employee owned devices clearly specified.

Make this information easily accessible e.g. in knowledge systems and on the intranet. Keep it forefront of mind by regularly checking understanding through audits or surveys and making it a requirement for employees to sign a letter of understanding on an annual basis.

Manage the demand and ensure sufficient capacity of computing for those employees not adopting BYOD and for the instances where employee owned devices are not able to operate.

Equip the Service Desk and support teams with the skills, tools and knowledge to support the myriad of devices entering the organisation. Make it clear to the Service Desk and support staff, as well as employees, the scope and boundaries of support provision for employee owned devices.

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.

Finally, embrace it, love it, and cherish it. BYOD is all about happy, empowered, enabled and productive employees. BYOD is about the ability to attract, engage and retain our talent. Don't we all want that?

Acknowledgement – Thanks to John Custy (@ITSMNinja) for his feedback on the initial release of this article and suggested improvements.

Karen Ferris is a Director of Macanta Consulting Pty Ltd and can be contacted at Karen.ferris@macanta.com.au.