The BYOD Revolution Means ITSM Evolution

How ITSM Needs to Change to Support BYOD

Karen Ferris

ABSTRACT

The adoption of Bring Your Own Device (BYOD) practices in the enterprise is gathering momentum. By 2016, Gartner predicts 38% of companies will have stopped buying devices for employees; by 2017, half of employers will require their employees to supply their own devices; and by 2020 85% of companies will have some sort of BYOD program. This paper explores how IT Service Management (ITSM) can support the BYOD movement and also what the emerging trend means for ITSM.

INTRODUCTION

BYOD is no longer new but it is still a subject that is being written about prolifically.

Recent research by Gartner estimates that by 2020, 85% of companies will provide some sort of BYOD program.

By 2016, 38 percent of companies expect to stop providing devices to workers.

By 2017, half of employers will require their employees to supply their own devices.

Forrester research predicts that over 70% of mobile professionals will conduct their work on personal smart devices by 2018.

Despite the security concerns, which I will touch on later, a key driver for BYOD is the benefits it brings.

Last year (2013) the Australian National Audit Office (ANAO), an independent government agency that oversees 300 agencies and reports to the country's parliament updated and modernised its mobile infrastructure. ANAO reports that productivity has risen by around 20%, which overall staff satisfaction rates have climbed by 15%. Gary Pettigrove, ANAO's CIO, is quoted as saying:

"Mailboxes are smaller, people are responding faster and employees say that they have better work-life balance. We're a quicker, smarter and more efficient organisation".

It is also better for the workforce, particularly when access is needed for a diverse range of people including remote workers, contractors and outsourcers. It can lead to significant savings on both capital and operational expenditure. It results in a happier and more productive workforce who can work where they want, when they want and on devices of their choosing.

Another driver is Gen Y. They are entering the workforce and bring with them a unique core life experience. Most of them have grown up with laptops and mobile devices and are accustomed to being connected to information – and one another – at all times. They have an expectation to choose to use what device they use to do their work. An organisation's adoption of BYOD will affect their ability to attract and retain talent.

According to CIO.com:

"Millennials don't want to unplug from work on the weekends and after-hours like their older counterparts, and so they want technology that keeps up with this lifestyle. They're driving today's big tech trends, such as consumer tech and bring-your-own-device, or BYOD, which naturally blends work life and social life.

Truth is, they want to be in charge of the technology they use at work and don't want to be told otherwise. And chances are they do have a better grasp of the power of technology than older generations that grew up with, say, desktop computer towers, numeric pagers and clunky Microsoft Office".[1]

---

1 http://www.cio.com/article/716369/CIOs_Look_Ahead_Millennials_Consumer_Tech_and_the_Future

The fact is that if you try and deny BYOD access, tech-savvy workers will find a way around it and will still use personal devices for corporate email, document creation and sharing, presentations etc. Therefore you might as well embrace it and not fight it.

It may seem scary but IT has lived through this before and survived. We switched from mainframes and dumb terminals to desktop PCs in the 1980s and the rise of the Internet in the 1990s. Now its BYOD but we are already seeing the next thing in the commoditisation and consumerisation of IT. IT has to change and evolve just as does ITSM.

So what does BYOD mean for ITSM? This paper explores how the ITSM processes will need to evolve to support the BYOD revolution.

SERVICE STRATEGY

Strategy Management for IT Services

As always, it is important to align with the organisational strategy. IT needs to determine the organisation's business goals and priorities, including goals for future growth, employee enablement and technology innovation adoption. Then, plan out how a BYOD strategy could fit in and enable those goals.

A BYOD programme should not get initiated just because people want to bring their own device. There has to be a business driver such as increased productivity, cost savings, attraction and retention of talent etc.

In the Insight Enterprises paper "Achieving a BYOD (Bring Your Own Device) Strategy That Works for You" it states:

"The risks associated with implementing a BYOD strategy cannot be addressed just by implementing a Network Access Control device such as a firewall, or simply by developing employee rules or policies. To ensure security, compliance, and data protection, companies need to develop a seamless, integrated mixture of policy and procedure, network infrastructure and resources, and process and management. All of these factors must be easy to ***understand*** *and use by the range of employees and* ***flexible*** *to meet their needs".* [2]

Once it has been decided that BYOD is an integral part of the organisational strategy, the strategy for the BYOD service can be defined during the Service Portfolio Management process and documented in the Service Portfolio.

Service Portfolio Management and Financial Management

The Service Portfolio Management 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 to the organisation.

Questions that needs to be asked in order to define the BYOD service include:

- What employees, employee groups or user profiles need access?
- Does BYOD extend to consultants, contractors and partners?
- What types of devices will they have or need?
- What privileges or permissions do they need?
- What data will they need access to?
- What is the risk profile of the data?
- What applications do they need?
- What is the geographical location? Office, home, road?
- When will they need access to resources and which resources?
- What functionality do they need? e.g. initiate web conferences, run financial reports, access HR systems, access corporate directories, calendar meetings on a mobile phone etc.
- What integrations are needed e.g. CRM, ERP?
- What is the best way to engage employees to accommodate necessary modifications to their devices for security such as encryption or authentication?

[2] http://www.insight.com/content/dam/insight/en_US/pdfs/insight/solutions/5-steps-to-byod-white-paper.pdf?cm_re=Solutions-_-CYOD-_-5-Key-Steps-PDF

- How will devices be supported? Do we outsource support? Do we 'time-box' support in that support only spends so long trying to resolve an issue and after that the user is on their own? Do we only support commonly used devices?

Service Portfolio Management will also need to look at what will be contained within the BYOD policy. The trick – easier than it sounds - is to come up with common-sense BYOD policies that allow employees to use their devices without jeopardising security.

The reason I say that is because recent research of 3,200 employees between the ages of 21 and 32 (Gen Y demographic) revealed that more than half (51 percent) of the study's respondents stated that they would bypass any BYOD policy at work.[3] These workers were raised to consider access to information a right, not just a privilege.

Careful consideration also 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.

It is not the intent of this paper to go into the content of a BYOD policy in detail, but it should include who owns what applications and data; corporate access to data contained on a device, organisational right to wipe data in the event of device loss or theft; employee security responsibilities e.g. password protection; levels of support available; what happens when an employee leaves the company etc.

The policy also needs to consider local legislation. For example, if a company owned device is lost or stolen, the policy may be that IT can remotely wipe the device to prevent data loss. However, in many countries (e.g. South Korea, Italy, France and others) it is illegal for a company to wipe a device that it doesn't own.

The most important aspect of your BYOD policy is to ensure that everyone is educated about the reason for the policy. The Insight Enterprises paper describes this perfectly. Having developed your BYOD policy and strategy….

"Now is the time to educate employees about the reasoning behind the BYOD policy along with the fact that it is going to be enforced. It is very important that employees are aware of this for the implementation to be successful. Unfortunately, employees bring on a majority of security issues because they are unaware of the policy or choose to ignore or actively circumvent it.

Educating employees is especially imperative as the so-called Internet Generation enters the workforce. According to a Cisco Connected World Technology Report, seven out of 10 young employees frequently ignore IT policies, and one in four is a victim of identity theft before the age of 30. The report goes on to state that "the desire for on-demand access to information is so ingrained in the incoming generation of employees that many young professionals take extreme measures to access the Internet, even if it compromises their company or their own security. Such behavior includes secretly using neighbors' wireless connections, sitting in front of businesses to access free Wi-Fi networks, and borrowing other people's devices without supervision...considering that at least one of every three employees (36%) responded negatively when asked if they respect their IT departments, balancing IT policy compliance with young employees' desires for more flexible access to social

[3] http://www.enterprisenetworkingplanet.com/netsecur/is-gen-y-bypassing-byod-policies.html

media, devices, and remote access is testing the limits of traditional corporate cultures." [4]

Service Portfolio Management needs to ensure that the provision of BYOD as a service remains viable and where not, decide whether elements of the service can be retired.

Financial Management needs to investigate the cost of a BYOD service including Return on Investments (ROI) and Return on Value (ROV). 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 devices, 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, retention, satisfaction, and productivity.

Financial Management needs to consider aspects such as - who pays for the device usage? If an organisation only wants to recompense for work related calls and data, this could put a large burden on the financial team who will have to validate all claims. This poses a challenge to forecast and manage cash flow.

Business Relationship Management and Demand Management

Business Relationship Management (BRM) is crucial in the establishment of a BYOD service and determination of the business need behind why people want to use specific devices. Is it just a new fad or is there a real business driver? BRM should work with the business to look for business efficiencies and technology advances that can make jobs easier or provide benefit to the organisation.

Demand Management will be pivotal in determining the demand for the service? Where and when will the demand come from?

[4] http://www.insight.com/content/dam/insight/en_US/pdfs/insight/solutions/5-steps-to-byod-white-paper.pdf?cm_re=Solutions-_-CYOD-_-5-Key-Steps-PDF

SERVICE DESIGN

Design Coordination

Design Coordination needs to drive consistent design of services and in a BYOD environment should be ensuring that applications are not designed for the desktop / web with mobile as an afterthought. Designing for mobile first and making sure the best layouts are in place for controls and functions will lead to a more engaging experience for users. It also allows designers to take advantage of mobile device's native features such as location-based services.

For example, Flipboard disrupted the publishing industry when it focussed on creating a new reading aggregation service specifically designed for tablets. It was only after the application gained popularity that it was considered as a web interface.

Service Catalogue Management

The Service Catalogue can play a key part in the BYOD revolution. It can clearly describe the service and where to get additional information e.g. policy, and can also set parameters.

If you have decided that you will restrict applications that can be connected to a device, the Service Catalogue is where you put that information. Given a wide enough variety of options, employees may not see this as a 'restriction' but a 'choice'. Then it is perceived as their choice and not something imposed by IT.

This may also reduce the introduction of rogue applications (as the catalogue contains approved ones) but when they are introduced (and detected), the organisation has recourse as 'approved applications' are documented as such in the Service Catalogue.

There is a sense of structure to illustrate that someone did something they shouldn't do and action was taken accordingly. This could also discourage future occurrences.

Service Level Management

Service Level Management (SLM) will have to ensure that Service Level Agreements are very clear on what is supported on a person's own device and what is not.

SLM 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 Desk' 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).

Availability Management and Capacity Management

Availability Management needs to adapt to the BYOD environment. Services that previously only had to be available during office hours may now need to be available during "working hours" which could now be 24x7.

Availability Management needs to ensure high service quality and availability. It will need to ensure, in conjunction with Capacity Management, that the wireless LAN (WLAN) infrastructure can support growing numbers of mobile devices and bandwidth hungry, delay-sensitive applications, while delivering predictable connectivity and service levels, and high quality of experience

Availability and Capacity Management need to take into consideration the influx of additional devices on the organisations infrastructure. Network performance could suffer and may mean infrastructure upgrades to manage the change in access type and usage.

Capacity Management needs to regularly monitor usage and plan for growth and expansion.

IT Service Continuity Management

BYOD can have advantages for an organisation's Business Continuity Planning (and IT Service Continuity Management - ITSCM) as if employees can still access their communication and collaboration tools remotely, any disruption to business as usual can be reduced.

However, you need to reassess the risk that BYOD brings to the organisation. Organisations need to take a close look at all critical systems and their associated sensitive data to determine how risk has changed with the advent of BYOD. All threats that could affect mobile devices need to be identified and mitigated where necessary.

Information Security Management

Information Security Management (ISM) needs to find innovative security solutions to mitigate the risk brought with BYOD such as a unified container solution. Containerisation is a secure vessel, which houses company data separate to personal information on mobile devices, ensures safe network access and provides centralised management of devices.

Mobile devices can become a conduit for malware from rogue apps and unless data is encrypted in-flight, its susceptible to interception especially when the user is on a public WIFI network.

Mobile devices are just that. Mobile. They are easily lost or stolen. ISM needs to ensure that devices can be locked or data wiped. ISM needs to determine how business content on a device can be managed without invading employee privacy.

According to ITWeb.co.za, ISM needs to do more than just Mobile Device Management (MDM) and mobile application management and should focus on five pillars of mobile security.

- *Protecting data in the data centre, in transit and on the device*
- *Strictly controlling access of the users who utilise these devices*
- *Enabling mobile interrogation, access and denial*

- *Providing unified policy management*
- *Containerisation of data and applications to address the blurring lines between corporate and personal data and applications on devices.* [5]

ISM should also provide employees with one-click access to only the corporate applications and resources that they have the right to access.

Before access is allowed, ISM must ensure that any mobile device connecting to the network must have its security credentials – such as jailbreak, or root status (critical to minimise the risk of malware infection), device ID, certificate status, OS version etc. checked.

Supplier Management

With more and more mobile device management solutions, mobile application management solutions, mobile content management solutions coming to market and suppliers now offering enterprise unified solutions, Supplier Management needs to ensure that the right supplier(s) with the right solution(s) for the organisation are engaged.

ITWeb.co.za also says:
"Organisations should be asking some searching questions from their IT partners to ensure their chosen mobile access solution consolidates control of all Web resources, file shares and client-server resources into a single location, with central administration and a single rule set for all resources and access methods. Access control solutions are available which allow IT to quickly set role-based policies for mobile and laptop devices or users with a single rule across all objects. As a result, policy management takes minutes instead of hours".

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

---

[5] http://www.itweb.co.za/index.php?option=com_content&view=article&id=70596

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

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, 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 for the BYOD environment and choose the most suitable for the requirements of the organisation.

SERVICE TRANSITION

Transition Planning and Support

Transition planning and support process has to provide overall planning for the introduction of BYOD along with all other Service Transition activities and to coordinate the resources that will be required.

BYOD will require input from many parts of the organisation at various stages of the implementation and this will need close coordination as they will also be required by other projects in-flight e.g. HR, legal, finance, procurement, supplier management, security, business continuity planning along with all aspects of IT Service Management.

Change Management

If your employee on-boarding 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.

All RFCs will need to be assessed for impact on services that are now supported by BYOD. In conjunction with ISM, the Change Management process should evaluate new devices for access to the organisation's network and data in addition to request for new applications to access that data.

Devices should be evaluated using questions such as 'Is this an upgrade to an existing device?' – that is - Is this a device that you already manage? If it is, does the latest version change something fundamental? If it is similar enough, then the device likely has the required security controls and is already supported in areas such as access control, authentication, MDM, data encryption etc.

As mentioned in 'Business Relationship Management', a request to connect a new type of device should be evaluated to determine the business need and ensure it is not just a new fad.

Service Asset and Configuration Management

In conjunction with other processes that need to protect the organisation from the risks of BYOD, Service Asset and Configuration Management (SACM) should treat BYOD devices just like any other device on the network. There needs to be an understanding of the native configuration and how to manage any necessary changes.

Jeff Wayman writing for ITSM Lens suggests the following use of the SACM process.

"1. Evaluate BYOD Processes – take a good look at what devices you already support. Consider asking questions like, "How often do we receive requests to allow Internet access for a tablet or smart phone?" and "Which employees benefit most from BYOD?" Finally, be sure to include a process for identifying or discovering new devices. Don't wait around for someone to tell you've they've started bring their own

device. You should know the moment they do.

2. Implement Automatic Discovery – most modern CMDB solutions will provide an automatic discovery tool. These can be configured to detect and notify you when a device has attached to your network for the first time. Be proactive and aware of how these devices are configured, the impact the pose to your organization, such as Internet bandwidth.

3. Monitor Potential Threats – While in the beginning mobile device were free from the potential for viruses and malware, this is starting to change. Latest research shows Android devices as the biggest target, but any OS can have security vulnerabilities. Given Step 1 and 2, make sure you have a procedure in place for making sure devices that come onto your network are up-to-date, and free of any unsupported software.

4. Conduct Regular Audits – Your CMDB will show you a historical record of devices that have attached to your network, as well as any changes that may have been made. Make it a point to regularly review this information". [7]

If you are recording employees as Configuration Items (CIs) on your Configuration Management Database (CMDB), 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.

Release Deployment Management & Service Validation and Testing

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.

Service Validation and 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.

[7] http://blog.sunviewsoftware.com/2012/01/5-steps-to-better-manage-byod-with-your.html

Change Evaluation

Change Evaluation is concerned with value and should ensure that the predicted value and benefits to be delivered by the BYOD program have indeed been obtained. The introduction of BYOD as a service is a major undertaking and therefore Change Evaluation is paramount if ROI and VOI are to be validated.

Change Evaluation will understand both the intended and unintended affects of the BYOD change.

Change Evaluation will provide the intelligence to inform future changes and additions to the BYOD service and will provide this information to Change Management for service improvement.

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.

SERVICE OPERATION

Event Management

Alerts and notifications to the employee and the Information Security Management team upon security violations should be automatic and corrective actions pursued. Therefore Event Management needs to incorporate alerts and events from BYOD and ensure they are routed to the area of the organisation best equipped to deal with them immediately.

Incident Management and Request Fulfilment

Both the Incident Management and Request Fulfilment processes will need to change to accommodate BYOD. The Incident Management process will need to ensure that Incidents related to specific devices get assigned to either an internal support group or a third party support capability depending on the device type. There will need to be clear definition of the support available for devices, connectivity, applications etc.

Standard request models should be defined that will generate standard changes for connectivity of pre-approved devices in a timely manner.

Service Desk

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

Liz Tay writing in IT News[8] 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.

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

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.

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.

Problem Management

As with any other service, Problem Management should identify and eliminate any recurring Incidents in relation to BYOD. Problem Management will work closely with ISM to ensure that the impact of security related Incidents that cannot be prevented are minimised.

Access Management

Access Management has to support the Information Security policy, processes and procedures put in place by ISM. This includes ensuring that employees only have access to corporate applications and data for which they have been approved.

Access Management will need to focus on right identify and authentication.

Access Management should also perform real-time monitoring of data access and audit trails to help contain risks associated with BYOD.

CONTINUAL SERVICE IMPROVEMENT

The Seven-Step improvement Process

Continual Service Improvement (CSI) and the Seven-Step Improvement Process needs to ensure that the BYOD environment within the organisation is subject to CSI as is any other service provided.

The BYOD strategy should be regularly examined to ensure it is fit for purpose. CSI should be proactive in driving proactive analysis of emerging trends that will either positively or negatively impact the BYOD plan.

Metrics should be established at a service, technology, people and process level and reported upon on a regular basis to identify any trends and ensure that BYOD is bringing the expected benefits to the organisation and risks are still being minimised.

CONCLUSION

As organisations 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, Service Design, Service Transition, Service Operation and Continual Service Improvement that it warrants.

The key is to clearly define the BYOD strategy and the BYOD policy. It then needs to be clearly and consistently 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?

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