BYOD, is the big bad wolf dead?

www.censornet.com

BYOD, is the big bad wolf dead?

Bring your own device (BYOD) is far from a cutting edge term, in fact, it's been on the table for a while now and it all started with the boss when they bought their nice new shiny toy into work that they got for Christmas and announced this is what they will use from this day forward.

The gospel according to BYOD had been born.

It became the universally accepted hall pass for 'Let's sidestep the policies we once insisted were important. Never mind that standardisation malarkey, details, details. Let's not worry about any of that, we have new shiny toys. That's all that matters'.

Of course, it's not just the boss any longer; we're all guilty. As the concept of BYOD began to grow a set of legs, the era of the smartphone and the tablet emerged and eye contact slowly became a thing of the past.

In May 2013, Gartner published an analyst view that, by 2017, up to 60% of businesses will have adopted a BYOD policy of some description. BYOD as a strategy may well prove to be an answer to many questions being posed to businesses the world over but do we now consider it a safe option?

In this white paper, we examine todays rationale for BYOD and try to answer the question; Is BYOD really a viable option and has that big bad wolf been tamed and transformed into an 'App shaped pocket sized pampered pooch'? It's a very good question.

Contrary to the hype, the speed of digital surprised everybody

There can be no argument that the digital world is rapidly changing at unprecedented speed. For many CIO's it really is a question of adapt or be left behind by the business they aim to support. We no longer care what the badge on the software says or who the vendor is in most cases. Many business users have grown up knowing nothing else but digital technology and all that it offers. They see the IT market as a supermarket; its shelves full of packaged services and products that they can choose for themselves. After years of exalting the virtues technology could potentially deliver, the hype has become the reality.

An IT department is increasingly being perceived as an organisation that introduces unnecessary delay. Obstacles previously regarded, mainly by a protective CIO, as barriers to technology adoption, are either being brushed aside or aggressively challenged by an ever-savvy user community. The fact is that the digital children are just as, if not more, familiar with the new technologies than many of their IT counterparts.

You're more likely to hear 'I'm going to anyway', rather than 'May I?' because that way, the job gets done but at what cost?

Where there is Wi-Fi, there's a way

By the very nature of digital channels, the need to always be on premise in order to undertake the duties of a specific job function has all but disappeared. Access to any site can be accomplished from almost anywhere that has decent WiFi signal. The number of devices that can facilitate access is considerable; smartphones, laptops and tablets all provide a means by which routine and sometimes complex, business processes can be undertaken.

The natives of this ecosystem regard your location as irrelevant to what you can do and when you can do it. Boundaries between work time and non-work time are now blurred owing to the ability to jump onto a mobile device, fire up the portal of choice and just get stuff done. You need only ask your spouse how easy it is to work from anywhere, as long as you remember to duck simultaneously.

The proliferation of devices seems almost unstoppable and the desire of workforces to exploit them is stronger than ever. Most analysts believe that any given individual will use at least three different devices during any given day. They'll typically include a laptop, a smartphone and a tablet, each potentially running three different operating systems, namely Windows, IOS and Android. Tablets, hybrids and laptops provide perfectly usable keyboards, many providing fold-away keyboards as standard, such as Microsoft's Surface Tablet.

The growing case for BYOD

Most new systems are designed with mobility as a given; it is now considered 'cards at the table'.

However, the ongoing consumerisation of IT is creating a shadow IT community and it is a planet over which CIOs have little or no control. Internet services, cloud applications and cloud storage are all options that enable businesses to create an elastic technology framework that they can exploit. Adopting BYOD, whether that's 'bring your own computer', 'your own phone' or even 'your own technology stack', makes simple economic sense.

BYOD so far has delivered in abundance:

It has left a big dent in capital costs

Firstly, it clearly reduces spend on hardware. The cost of purchase, replacement and general day-to-day management of hardware becomes the responsibility of the owner.

Staff acquisition and retention

Advertising that a business has adopted a culture of BYOD is to suggest that it is a fun and flexible place to work. Companies that openly encourage freedom of choice are seen as progressive.

Performance and productivity

Encouraging employees to use their own devices creates an environment in which they can work outside the corporate perimeter as much as within it. People naturally tend to take advantage of the work anywhere, anytime paradigm as they can interweave their social and work life far more effectively.

The net result and benefit for the company are that it becomes highly likely that they will work beyond contracted hours. Given the use of portals such as Google's Play store or Apple's iTunes the creation of a company portal plays on the personal experience of using these commercial portals because well, why not?

The opportunity for increased productivity is enhanced without any pressure from the employer.

Because we know best, that's why

Digital savvy employees are quick to adapt to new applications. They are also quick to identify what works and what doesn't. Input into process improvement increases so that it is no longer the sole domain of the business analyst. This encourages a community spirit, makes the job of the business analyst easier and can reduce the time it takes from innovation to deployment. In the coming decade, the emphasis on process innovation will be more important than the technology.

The interesting benefits of self-service

The expectation of Self Service seem equally to have risen and a given, rather than a 'nice to have'. The more a user can do for themselves, without redress to IT the better. Use of personal devices is just part of providing a more self-service orientated ethos. Employees have their own tools with which they can do their job. It is also a quirk of the digital world that self-help communities and forums tend to arise.

The perceived risks of BYOD – Have they really changed?

The poor old IT department, if there were ever an Olympic sport where you could count the moments between suggesting that technology could change the world and then having it bite you on the backside by an unruly mob, well, they'd be gold medallists.

Naturally, an IT team is predisposed to focus on the challenges and risks that a BYOD culture can bring, which is not a bad thing. In the IT world, BYOD makes the world a more complex place rather than a simpler one. A fixed desktop located on an internal network is always going to be simpler to deploy, easier to manage, easier to secure and much easier to monitor. The risks can be easily identified and mitigated.

The problem with browsers

With a few exceptions, the main browsers tend to be Chrome, Internet Explorer, Firefox & Safari. The problem arises when every user's personal device needs its browser software up to date. Take your fixed, standardised, controlled infrastructure away and it's not quite as easy. Some applications will simply not work on older browser versions or even with specific browsers. The quality of user experience may be compromised if the right browser is not selected. It can be a fickle, inconsistent way of working.

More importantly, not keeping a browser up to date may expose security flaws that place the device and its content at risk. Many have learned that particular lesson the hard way.

Our old nemesis 'malware and spyware infection'

The natural by-product of an increasing tech savvy world is that the bad guys are getting smarter and the users are more 'click-happy', particularly on mobile devices.

Users are seldom intentionally malicious, although clearly it happens. However it is often more a case of due diligence when time is a constraint. Not all will adopt sensible security protocols to ensure they are free of Trojans and other malicious autobots that might be hiding within what, at the time, looked like a cool free widget or an article containing a part of Kim Kardashian that broke the internet.

In 2013, a study by Alcatel-lucent in 2013 estimated that 11.6 million devices were infected; a number that is simply likely to grow. The fastest growing infection rates was on Android with Windows and Android being the primary operating systems likely to be targeted.

In Wi-Fi we (don't) trust

All mobile devices will invariably hop on and off Wi-Fi with reasonable regularity. The bandwidth and access point will play a role in mitigating the risk of contamination. Using unsecured hotspots increases the risk,

not only to the user but potentially the corporate network. The bad guys are smart and unsecure access channels are a happy hunting ground. An experiment by Jonny Milliken, Valerio Selis and Professor Alan Marshall proved that an airborne virus could be transmitted via WiFi from router to router and hence from one device to another. The attempts to access precious data are unrelenting on the increase.

Even on-premise WiFi can be problematic. The strength of any WiFi and available bandwidth may well dictate how usable a commercial application is on any given mobile device. It should be remembered that not all devices have the same capabilities when it comes to transmission and reception.

Authentication

The mechanism of accessing corporate applications, network and resources requires a method of authenticating that the user is who they say they are. Inadequate mechanisms open the door to abuse.

Legal constraints

It may not immediately spring to mind, but a business cannot control the peccadillos of its employees. A personal laptop that has been used for social activities that cross legal boundaries is one that can compromise the integrity of the business and all that could entail. Reputation is as much a protected treasure as any other business asset, as is consumer confidence in who they are buying from.

Data loss

The most precious asset of any organisation is data. Sales prospects, agreements, policies, goals, strategies, Financial Information, Shareholder reports, whatever information an organisation has must be kept secure. The ramifications of data loss can be severe. A user's device can compromise data in a variety of ways and not just from pernicious access. How much and where on a device is corporate data going to reside? What degree of sensitive data can be trusted to be on a specific users' device? What about access codes? Is a user storing key account details in plain text somewhere? What happens if a device is lost or stolen, can data leakage truly be prevented?

Device control

If the device belongs to a user, do they have complete administration rights over their device? The owner tends to know how to use their device and how to change configurations. One potentially damaging scenario is if a user decides to jailbreak their own device so they can access areas that companies like Apple would rather they did not. Android also has its challenges, although not exactly open source, it naturally lends itself to modification and user changes, given its Linux roots. There is an ever-growing community that seeks to either legitimately change code or simply break it because it can be broken and compromised.

Application conflict

What a user downloads onto their own device is by and large a matter for them. Some applications however, particularly apps for smartphones and tablets, can interfere with commercial applications. There is no way that an IT department can track and recommend, from the hundreds of thousands of apps available, which ones are suitable or which could cause cross-application contamination i.e. result in sub-optimal performance or use.

Human error

No matter what technology is used, there is no way of avoiding simple stupidity or oversight by human beings. A human interface is a flawed one simply because we make mistakes and because the users own their devices; mistakes will inevitably happen. Human error will always be the one true constant why there is no such state as 100% secure.

From an IT standpoint, BYOD presents a raft of obstacles. They are challenges that can be met but the solutions are not foolproof and an element of risk will always remain.

It should be remembered that most security breaches are instigated by employees not cyber thieves. In 2014 a survey by a US institute (Ponemon – a think tank dedicated to advancing responsible management of information) indicated that data loss across US firms costs an average of $3.5 million per year.

The breakdown of the information loss is sobering read:

- *39% - confidential business information*
- *27% - customer data*
- *14% - intellectual property (IP) such as computer code*
- *10% - employee data*

It's all about governance

So, can a business manage applications on a multitude of mobile devices to limit the risk and let the benefits of BYOD live and breathe in a way that can really work in the real world?

There's one decent starting point that is easy to gain consensus and agreement - governance. Whichever sphere of IT is being studied, the presence of good governance, as opposed to weak or no governance, is a good indicator of how seriously an organisation takes risk mitigation and asset management. Good governance is about developing policies and protocols to align with business goals. It is about managing data, resources, the IT estate and business processes in a way that enables safe use and aligns with business goals to maximise value from assets, all without placing handcuffs on the user community.

Many IT departments opt for informal policies even if their organisation has ISO 2701 accreditation (ISO framework for information security management). It is not uncommon for organisations to tick the boxes for accreditation but then pay lip service to what that accreditation stands for. Good governance is not about lip service, it is about achieving a balance between protecting the company assets and facilitating ease of use for their employees.

Taming the Big Bad Wolf

So the reality is, the days of us saying "Oh my, what big teeth BYOD has" are probably over, not because the issue of risk has been solved entirely but the digital world is maturing and so must our approach to mobilising the value it can potentially bring. There are ways to ensure that it limits the opportunity for the wolves lurking in the digital forest just waiting to devour your crown jewels and still deliver clear tangible business benefit.

Scope it like you mean it

As with any undertaking, planning is vital. It also worth remembering that not all devices are made equal and focusing on a few core products will make it easier to manage in the initial phases. Start small and expand once the issues arising from the initial phase are resolved:

- Decide what information or data you must protect and control access to
- Decide which devices accessing that information or data are controllable given what we know about todays market
- Review which operating systems are in and which are out
- Identify a key part of the business that may see immediate benefits from BYOD
- Look at a few trusted employees who can act as part of a proof of concept exercise (POC)
- Identify the software and licenses required to implement BYOD
- Decide how devices will be monitored and by whom
- Consider using company devices in a POC before deploying to employee personal devices
- Review which technical skills are required
- Pick a suitable application to deploy that will pose less of a security risk

Define a policy

One important step is to defining what a BYOD policy looks like. It is best thought of as extending and enhancing web policies that prevail, assuming a company has any, within the perimeter of the organisation.

- What are the liabilities of the company and what are the liabilities of the employee?
- Can the policy be legally enforced?
- What happens if a device is stolen? Who is incumbent to do what?
- If data is lost will the employee be liable for a fine or disciplined and how will the rules around that be defined e.g. what defines culpability on the employee's part?
- How will the standing orders of the Data Protection Act be enforced?
- What will an employee have to agree to i.e. installing of monitoring software, security protocols etc. on their personal devices?
- Are there any restrictions on private apps that are known issues and can these be defined as deal breakers in allowing specific employees to take up the BOYD opportunity?
- What about private apps on the corporate network? Are they allowed or is a complete ban required?
- How is data to be managed?
- Are there minimum specifications for the devices e.g. must have 'n' gigabyte capacity?
- Is there to be a compensation package for using personal devices, such as when an employee breaches their providers' data limits?
- How is personal data protected from corporate access?

Create support guidelines

Support guidelines go hand in hand with any policy. Having access to both the policy and support protocols is a must, especially considering these are devices that may be functioning across the Internet. Guidelines need to be simple, clear and easily accessed. If a user has issues, the more they can self-diagnose the better. After all, they may well understand the device in more detail than the IT support services.

Acquire the right software

There are software options that will facilitate ensuring management of a BYOD paradigm is less fraught with issues, particularly around security of data. Knowing the user will inevitably resist any new form of software on a personal device, the reality is that the solution needs to be network based if it is to be successful.

Protection also doesn't mean prohibiting the user but the ability to identify, capture and manage any unusual activity that may compromise the organisation through use of a personal device. There is a fine line between an invasion of privacy and an airtight solution that protects the integrity of company data.

Conclusion

BYOD may not be a fresh term but we need to recalibrate the way we view and secure it.

Few of the traditional security arguments have changed and even fewer of the security vendors have taken into account that change which means they're probably 12-18months from being useful at any meaningful level.

It's no surprise that there has been an emergence of Cloud Application Control Providers or Cloud Access Security Brokers of late, technologies positioned to plug the gap of the vicarious user that is hell bent on productivity at all costs. It's an important step towards radically diluting the case against BYOD heralding a security risk.

"By 2016, 25% of enterprises will secure access to cloud-based services using a CASB (or CAC) platform, up from

less than 1% in 2012, reducing the cost of securing access by 30%" - Gartner – The Importance of Cloud Access Security Brokers.

The exponential rise of the App means that we're discussing less what risks BYOD carries and more about what learning's we can take from the last five years to cope with all that data growth and the cloud have presented. Applications intended for the Enterprise Market will almost certainly contain security consideration at a basic level but are often aimed more at making our lives easier, therefore naturally carry the risk of fallibility.

As more companies seek to embrace cloud applications to replace in-house legacy systems, it's easy to miss the blindingly obvious. Apps are generic by definition; they are created to service a mass market and therefore the security considerations are broad and lack granularity, therefore the natural by-product creates unnecessary risk.

If security and privacy requirements are to be meaningfully applied, the business needs greater visibility and control of enterprise data in the cloud that is accessed using unmanaged devices. It needs to identify risks as they occur, not act as a forensics tool for after the event.

The days of pointing at the cloud provider if something goes wrong died a long time ago, if indeed they ever had a life. Users will find their way around any policy to get the job done, so the challenge remains to transparently enforce security policies without intervening in the end user experience that people have grown to enjoy from cloud applications and related services.

The need to educate and govern users will never go away because they're proven to be spectacular at breaking the rules that are designed to protect them.

Modern Cloud Application Control should have the ability to change BYOD from a well-meaning concept to an applied business friendly policy if they truly 'follow the user'. It should enable the discovery of all cloud apps and services, assess the risk and be able to audit and log all usage, maximising visibility for everyone's benefit beyond simply reporting after the event.

If we embrace the current merits of traditional web security and content filtering but shift our focus to the user, tracking unusual or suspect behaviour becomes a far simpler task. The risk of 'What device' or 'Which application' becomes a greatly diminished variable risk if you combine proven web security and content filtering with the advances that Cloud Application Control functionality brings.

The approach to security will ultimately be a matter of choice based on a robust risk assessment. Web security has to evolve to also deliver visibility and control of cloud apps in addition to the traditional way of content filtering, data, URL's and virus scanning.

There also needs to be an acceptance that some personal data may well leak back into the corporate network. This may appear unacceptable to some, but already employees use social media within the corporate perimeter and they already propagate social data via email or various chat software. An employee's life is no longer delineated. The mere fact that smartphones exist has meant that social communication is a daily fact of life for most employees, be it via Facebook, Twitter or simple SMS.

A continual blurring between the lines around what is work and what is not has been taking place for the past decade, so we can't pretend to be surprised. It will only continue to merge as the technology improves. Understanding and accepting this landscape is critical to the success of implementing a BYOD policy, just as acquiring the right tools to manage and monitor the multitude of devices is.

It must always be remembered that if there is a Big Bad Wolf stalking your assets, a silver bullet is never going to be guaranteed. The rise of Cloud Application

Control significantly mitigates the traditional risks posed by BYOD. They enjoy smaller unobtrusive footprints invisible to the user but act intelligently to follow and understand the activity; keeping themselves and the organisations they work for in a far healthier secure state of mind and working.

BYOD as a concept or an acronym has enjoyed a decent shelf life but the security uncertainties that accompany it have eroded and are fast becoming yesterday's concerns. The barriers to adoption are diminishing and the mitigation of security risk is there for progressive companies that are willing to trash technology that was designed and architected to serve the market challenges of BYOD a decade ago.

Erecting a picket fence outside Windsor Castle and calling it a deterrent is probably not the most credible protection system. Traditional web security and filtering products were not designed to cope with today's vast number of mobile devices and cloud applications, they need to evolve to embrace and show clear Cloud Application Control capability if they are to effectively serve today's digital world.

In the absence of that progression, if BYOD is a serious consideration for you, then ignore the importance of monitoring, managing web access, application usage at your peril but ensure that your web security technology has Cloud Application capability; otherwise, one day soon you'll be fresh out of excuses.

CensorNet | Powerful, enterprise-class cloud security for your organisation

Secure Web Gateway

CensorNet Secure Web Gateway (SWG) is our next generation web security solution with built-in Cloud Application Control capability and the power to extend web access policies to Bring-Your-Own-Device (BYOD) initiatives.

Hybrid Web Security

CensorNet Hybrid Web Security (HWS) platform offers the best of both worlds - the security and control of an on-premise or endpoint component, together with the flexibility and mobility of a centralised cloud service.

Email Security

CensorNet Email Security is a cloud based email security and backup service that scans both inbound and outbound email for viruses, phishing threats, content violations and spam.

Desktop Monitoring

CensorNet Desktop Monitoring is a client-server solution for monitoring, recording and analysing user activity on the desktop, virtual desktop, terminal services and remote desktop sessions.

Company Head Office
Network House . 6th Floor . Suite 6.01
Basing View . Basingstoke . RG21 4HG . UK

Research & Development Centre
Bristol & Bath Science Park . Dirac Crescent
Emersons Green . Bristol . BS16 7FR . UK

t: +44 (0) 845 230 9590
f: +44 (0) 845 230 9591
www.censornet.com