BYOD&ndash;The Hottest Trend or Just the Hottest Term

Peter Silva, 2012-05-04

It goes by many names: ‘Bring Your Own Danger’, ‘Bring Your Own Disaster’ and what most people call ‘Bring Your Own Device’ and everyone it seems is writing, talking and surveying about BYOD. What used to be inconceivable, using your own personal mobile device/smartphone for work, is now one of the hottest trends or at least, one of the hottest topics being discussed throughout the IT industry. The idea of using a personal smartphone at work sprouted, I think, when many executives got their first iPhone back in 2007 and wanted access to corporate resources. As more smartphones made their way into employee’s hands, the requests for corporate access only grew. Initially resistant to the idea due to security concerns, IT seems to be slowly adopting the concept based on the many blogs, articles and surveys that have littered the internet of late. But, it is a true trend that will transform IT or simply a trending term getting a lot of attention? We’ll be right back after these important messages.

Just Kidding. Most likely the former.

While many of the cautionary articles talk about potentially grim disasters, they do acknowledge that BYOD is not going away and in fact, is gaining ground. Greater productivity and cost savings seem to be the driving factors. Let’s take a quick look at the smattering of articles surrounding this offshoot of IT consumerization.

The Mobile Device Threat: Shocking Mobile Security Stats: A nice slide show featuring highlights from a recent Ponemon Institute and Websense survey. Right out of the gate they talk about how mobile devices are a double-edge sword for enterprises. 77 % of the 4640 responses said that the use of mobile devices in the workplace is important to achieving business objectives but almost the same percentage - 76% - believe that these tools introduce a "serious" set of risks. While organizations understand the risks, the survey showed that only 39% have security controls in place to mitigate them. As a result, 59% of respondents said they’ve seen a jump in malware infections over the past 12 months due, specifically, to insecure mobile devices including laptops, smartphones, and tablets while 51% said their organization has experienced a data breach due to insecure devices. While 45% do have a corporate use policy, less than half of those actually enforce it. In terms of recommendations based on their findings they said, be sure to understand the risk that mobile devices create in the workplace; educate employees about the importance of safeguarding their devices; create a mobile device corporate policy and leverage mobile device management solutions, security access controls, and even cloud services to keep confidential data out of the eyes of unauthorized viewers.

10 myths of BYOD in the enterprise: A nice top 10 from TechRepublic primarily pulling data from a recent Avanade survey of more than 600 IT and business leaders. The notion of IT resistance to BYOD is somewhat squashed here with nine out of 10 respondents (according to the results) saying their employees are using their own tech at work. They found that more Androids are encroaching the workplace; that employees are actually using it for work rather than playing games and that nearly 80% of enterprises will make investments this year to manage consumer technologies. There’s 7 more myths along with a couple nice graphics to go along with the list. Interesting and quick read.

When Business and Personal Combine: This Wall Street Journal article talks specifically about the conundrum companies and employees face when a remote wipe comes into play. What happens, or really, how to deal with situations when there is a fear of a data breach yet wiping the device also deletes all the employee’s personal data, like family pictures. Policies, use agreements and mobile device management (MDM) solutions are potential solutions.

The new BYOD: Businesses are now driving adoption: Rather than the perils of BYOD, this InfoWorld article talks about how enterprises are starting to actively encourage BYOD, not just passively accept it. Reporting on Good Technology's recent BYOD survey, they found that organizations are jumping on the phenomenon sine they see real ROI from encouraging BYOD. The ability to keep employees connected (to information) day and night can ultimately lead to increased productivity and better customer service. They also found that two of the most highly regulated industries - financial services and health care - are most likely to support BYOD. This shows that the security issues IT folks often raise as objections are manageable and there's major value in supporting BYOD. Another ROI discovered through the survey is that since employees are using their own devices, half of Good's customers don't pay anything for the employees' BYOD devices – essentially, according to Good, getting employees to pay for the productivity boost at work.

BYOD Is The Challenge Of The Decade: Europe is also seeing the BYOD trend. This TechWeek Europe article talks about the familiar threats of malware, spyware, worms and other malicious software but also says that BYOD success depends on both people and technology. That it's important to involve management early, consider the legal and financial ramifications along with risks to the business to then make an informed decision about a BYOD plan. Not sure if it's the challenge of the decade but it's a great headline and will continue to fluster IT in the coming years.

IT Security's Scariest Acronym: BYOD, Bring Your Own Device: This PCWorld article uses Nemertes Research data to cover the discrepancies between how companies treat laptops (which can be mobile) and mobile devices themselves. They both have VPN capabilities and device encryption available but stray in different directions after that commonality. The obvious difference is laptops are usually IT owned and smartphones are personally owned. They suggest that it's a good idea to re-evaluate the difference between security controls on different types of end-user devices and ask, "*Is this difference based on valid reasons or a result of legacy thinking*?"

BYOD Challenge: How IT Can Keep User-Owned iPhones And iPads Secure In Enterprise: This article looks at both the technical and personal challenges to securing employee-owned devices along with suggestions like user education, cost sharing, purchase assistance, tiered access, reward for enrollment and reward for good behavior. I like the last one since much of our challenges and much of what I write about is human behavior, the human condition and why we do the risky things we do.

BYOD: Manage the Risks and Opportunities: Bankinfosecurity.com is one of my weekly stops on the internet circuit. While this article is more a primer for an upcoming webinar, it does offer a number a good questions to ask while considering a BYOD strategy. They also say that it's no longer a question of whether to allow employees to use their own devices – the questions are now about inventory, security, privacy, compliance, policy and opportunity.

Some BYOD thoughts based on all of the above, in no particular order:

- Have a BYOD policy or forbid the use all together. Two things can happen if not: personal devices are being blocked and organizations are losing productivity OR the personal devices are accessing the network (with or without an organization's consent) and nothing is being done pertaining to security or compliance.
- Ensure employees understand what can and cannot be accessed with personal devices along with understanding the risks (both users and IT) associated with such access. What's the written policy and how is it enforced. Acceptable use.
- Ensure procedures are in place (and understood) in cases of an employee leaving the company; what happens when a device is lost or stolen (ramifications of remote wiping a personal device); what types/strength of passwords are required; record retention and destruction; the allowed types of devices; what types of encryption is used.
- Organizations need to balance the acceptance of consumer-focused smartphones/tablets with control of those devices to protect their networks.
- Organizations need to have a complete inventory of employee's personal devices - at least the one's requesting access.
- Organizations need the ability to enforce mobile policies. Securing the devices.
- Organizations need to balance the company's security with the employee's privacy like, off-hours browsing activity on a personal device.
- Personally, I do find that if I'm playing a game at 9pm and an email comes in, I typically read it.

F5 has a number of solutions to help organizations conquer their BYOD fears. From the Edge Client, to our BIG-IP Global Access Solutions (BIG-IP APM and BIG-IP Edge Gateway) to the recent MDM partnership announcements, we can help ensure secure and fast application performance for mobile users.

ps

Related or, …and the Rest:

- The Dark Side of BYOD – Remote Wiping and Other Issues
- How do we manage the BYOD boom, at the technical end?
- BYOD: Bring your own device could spell end for work PC
- Bring Your Own Device: Risks and rewards
- What Risk Does 'BYOD' Pose To Your Business? Survey Says
- Mobile Device Security Threats Attract Cybercriminals
- The BYOD Security Dilemma
- BYOD and the hidden risk of IT security
- BYOD Policy Template
- Secure iPhone Access to Corporate Web Applications