# Bring Your Own Disaster! Warning. BYOD is still a risk for company data and reputation

Submitted by: Kiss Communications
Monday, 29 October 2012

---

James Easton, Pre-Sales Consultant at IT modelling and data visualisation software company Real Status (http://www.real-status.com/), says that businesses allowing employees to BYOD (bring your own devices) to work risk unleashing a security/compliance nightmare. Many businesses allow employees to use their own smart phones, tablets, memory sticks or laptops while on company premises, but then fail to implement adequate security policies to police them.

A recent Ovum survey 1 showed that almost 80 percent of BYOD activity is inadequately managed by IT departments; nearly half of respondents were either not aware of BYOD activity or ignored its existence, by operating a “don’t ask, don’t tell” policy. Only 8.1 percent actively discouraged it.
Whereas traditionally a business’s IT security policy is set and implemented by an IT manager or the CIO, the use of BYOD effectively “crowd sources” it by opening up security management to everyone.

IT managers may not even know how many mobile devices are connecting to their networks. A 2011 survey2 estimated that 69% of employees used smart phones for work, whereas their respective IT managers estimated that only 34% did so.

James has outlined some of the perils and solutions to this growing problem:

1). Jumping the perimeter: viruses, malware, spyware and hackers can often “jump the security perimeter” – that is, when these are bought into the company, the data they send and receive does not use the border /perimeter security solution; they may also bypass the firewalls that monitor ingress and egress points of the network.

2). Patch management: security updates will not be consistently applied across all devices connected to the network. Security patch management is often underestimated and treated as an afterthought, but falling behind with even one update can allow a new virus or exploit to slip through without being detected by the anti-virus software.

3). Password security and encryption: will often be weak or non-existent. Every BYOD device should have data encryption, password protection and the ability to lock users out if there are more than three incorrect attempts to access it. Sloppy password control along with lack of encryption can lead to accounts being hijacked and the potential for serious loss.

4). Time management: businesses need to be aware of staff going onto Facebook, Twitter or playing with apps which would normally break ‘Acceptable Use Policies’ on company-maintained equipment. For example, the results of a 2010 Sophos survey, "Security Threat Report 2010"3, showed that 60% of firms polled, thought that Facebook posed the biggest threat to their security, well ahead of MySpace, Twitter, and LinkedIn. Users often use the same passwords for work and social media leaving data vulnerable.

5). Data privacy – what leaves and enters your network. As soon as BYOD becomes TYOD, or Take Your Own Device, data is vulnerable. For example, when employees share their devices or passwords with other

people, when their devices are lost or stolen or when data is accessed on unsecured networks or public Wi-Fi hotspots.

James comments:

“There are some basic security rules that should be implemented at minimum, but they are all dependent on individual employees being trusted to stick to them all the time. The only way that a robust corporate security policy can be implemented with any guarantee is for employees to allow control of their BYOD devices to be shared, monitored and maintained with their security team. But that in itself raises a whole new set of privacy, access and cost issues.”

---ends---

Editors’ Notes:

1. Ovum reveals firms face huge security risks as 80% of BYOD goes unmanaged http://ovum.com/press_releases/ovum-reveals-firms-face-huge-security-risks-as-80-of-byod-goes-unmanaged/ (http://ovum.com/press_releases/ovum-reveals-firms-face-huge-security-risks-as-80-of-byod-goes-unmanaged/)
2. http://blogs.unisys.com/disruptiveittrends/2011/07/12/one-year-on-too-many-it-groups-still-struggle-with-consumerization/ (http://blogs.unisys.com/disruptiveittrends/2011/07/12/one-year-on-too-many-it-groups-still-struggle-with-consumerization/) - (Dec 2011)
3. "Revealed: Which social networks pose the biggest risk?" (http://www.sophos.com/blogs/gc/g/2010/02/01/revealed-social-networks-pose-biggest-risk/) and http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf (http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf) - (1 February, 2010)

About James Easton

James has worked in the networking and security space for nearly 22 years. With extensive experience of working across the EMEA region from assembling early Cisco routers, Network Manager and then to Security Consultant, advising on security practices. He has held a number of senior roles including Sales Manager at Verisign (http://www.verisign.co.uk/), and various technical consultant and engineering positions at Arbor Networks (http://www.arbornetworks.com/), Cablefree Solutions (http://www.cablefree.co.uk/), Global Crossing (http://www.level3.com/) and Reuters Intertrade Direct.

Reporting to Stace Hipperson, Chief Technology Officer (CTO) at Real Status, James’ role is to present the company’s unique product Hyperglance (http://www.real-status.com/index.php?option=com_content&view=article&id=7&Itemid=122), the world’s first 3D modelling and visualisation software product which reveals every dimension of inter-dependence between applications and infrastructure, to customers.

About Real Status (http://www.real-status.com/)

Real Status is a leading software company, specialising in the modelling and visualisation of

infrastructure and IT applications, to enable enterprises to gain business context and insight. Their flagship product, Hyperglance, is the world's first IT modelling and visualisation solution that cuts through the complexity of modern IT systems to give enterprises a comprehensive, 3D view of their entire infrastructure and applications. To see an introductory video of Hyperglance, click here Privately owned and based in Cambridge, UK and San Jose, California, USA, Real Status was selected as one of GigaOM's Structure finalists in 2011 and one of SIIA's Next Gen Companies for 2012. Its customers include large organisations from the Financial, Government, Food Products, Transportation and Distribution, Manufacturing and Media industries.

For more information, please visit: www.real-status.com or follow Real Status on Twitter (https://twitter.com/hyperglance)

Laura Brown/Justine Smith
KISS Public Relations
T: + 44 (0)208 12345 75
E-mail: laura@kisscom.co.uk / justine@kisscom.co.uk