VOICE&DATA

Date – October 10th 2012

Risks and Opportunities around BYOD

The evolution of Bring Your Own Device (BYOD) trend has been as profound as it has been rapid. It represents the most visible sign that the boundaries between personal life and work life are blurring. The 9-5 pm model of working solely from the office has become archaic and increasingly people are working extended hours from a range of locations including the workplace, out in the field, during the commute, and from home. We truly live in a 24/7 global workplace and few people are surprised to receive business emails late in the evening.

At the very heart of this evolution is the ability to access enterprise networks from anywhere and anytime. The range of tools which enable this constant connectivity are becoming more powerful all the time, with laptops, tablets, and smartphones allowing access to a range of communications and business applications, while cloud computing serves to effectively extend the office out of the office.

The much-heralded benefit of BYOD is greater productivity. However, recent research has suggested that it may actually be the great myth of BYOD and the reality is that BYOD in practice poses new challenges that may outweigh the benefits, if it is not properly addressed by the organization.

A worldwide survey commissioned by Fortinet, a world leader in high-performance network security, chose to look at attitudes towards BYOD and security from the users point of view instead of the IT managers. Specifically, the survey conducted in 15 territories focused on graduate 20 something employees. This group represents the first generation to enter the workplace with an understanding and expectation of own device use. They also represent tomorrow's influencers and decision makers.

What all does the Survey Say?

The survey findings will concern both network managers responsible for security, as well as senior management ultimately responsible for the strategic decision about the degree to which the business embraces BYOD. For financial organizations, this decision becomes even more critical. Larger organizations will have mature IT strategies and policies in place. But what about smaller financial businesses that might not have such well developed strategies and for whom the culture of BYOD might already be established in the workplace? Should they be concerned about the behavior and attitudes of staff, especially younger employees?

Crucially, within this younger employee group, BYOD is predominantly considered a right rather than a privilege, with over half (55%) of the people sharing an expectation that they should be allowed to use their own devices in the workplace or for work purposes. With this expectation comes the very real risk that employees feel so strongly that they will consider ignoring company policy banning the use of own devices. More than a third (36%) of people polled admitted that they have, or would contravene such a policy. However, this latter statistic, worrying though it is, has noticeable geographic differences with India being the most risk-laden territory. An astonishing 66% of survey respondents from India admitted that they are willing to contravene policy.

The threat posed by this level of subversion cannot be overstated. For example, people are increasingly tech savvy and are able to set up their own smartphones to access work emails without assistance from IT departments. But with the Android OS being a huge growth area for malware, and with people using their smartphones to access social media such as Facebook (an increasingly dangerous environment), it quickly becomes obvious where the threats lie.

The survey casts doubt on the idea of BYOD leading to greater productivity by revealing the real reason people want to use their own devices. Only 26% of people in this age group cite efficiency as the reason they want to use their own devices, while 33% admit that the main reason is so they have access to their favourite applications. But with personal applications so close to hand, the risks to the business must surely include distraction and time wasting. To

Highlights

- For younger generation BYOD is considered a right than a privilege
- A survey says 36% workers are against banning of BYOD in office
- 66% Indians are against too
- 26% people cited efficiency as the reason to adopt BYOD

support this assumption, 46% of people polled acknowledge time wasting as the greatest threat to the organization, with 42% citing greater exposure to malicious IT and theft or loss of confidential data. Yet, even with this widespread understanding of the downsides to BYOD, only 27% believe the risks outweigh the benefits for their organization.

Clearly, from a user perspective there is a great deal of contradiction surrounding BYOD and an undercurrent of selfishness where users expect to use their own devices, but mostly for personal interest. They recognize the risks to the organization but are adamant that those risks are worth taking.

Need for a Policy Governing BYOD

So what of responsibility? This is a key question for any business considering a policy governing BYOD, as the challenge for the organization is to put in place security measures to ensure safe integration of user-owned devices. But to do that requires the cooperation of the device owner. The Fortinet survey suggests that gaining cooperation and compliance from employees might not be that straightforward.

66% of people polled considered themselves to be ultimately responsible for security on their own devices, with only 22% passing the responsibility to the organization. This would suggest that, while the owners are more than happy to use their own devices in the work environment, they might be highly resistant to any suggestion that the organization puts any limits on usage or interference with the device to install security measures.

The full extent of the delicate balancing act facing the organization is finally revealed with the statistic that nearly 1 in 5 people would consider holding back their own devices if they felt that the organizationâ??s security systems were so vulnerable as to pose a real risk to their own personal data. As far as the users are concerned, BYOD is something that they approach very much on their own terms.

BYOD is here to stay. While the Fortinet survey balances the widely held belief that BYOD is mostly beneficial to business by highlighting some key security challenges, it also shows that organizations must address the issue at the earliest stage if they are to extract any benefits from a practice that they will have great difficulty resisting. The most effective way to do this is by securing inbound and outbound access to the corporate network and not just implementing mobile device management. It is a dangerous strategy to rely on a single technology to address the security challenges. The strategy should be one of granular control over users and applications, on top of devices.

The reality is that technology consumerization is invading the workplace, but the organization cannot afford to simply stand back and let users have their way. It's time for the business world to stand its ground.

Vishak Raman
The author is senior regional director, Fortinet
vadmail@cybermedia.co.in