BYOD - A mixed bag

by Dr. Hemant Chaskar, VP of Technology and Innovation, AirTight Networks, USA

The BYOD (*bring-your-own-device*) trend is growing rapidly, but it is a somewhat mixed blessing for most organisations. Although BYOD policies are popular with employees and can also bring a variety of savings, they also can be costly, difficult to administer and present serious security risks. The wide variety of devices employees are likely to bring makes it difficult to administer network and data security, software and applications updates and, as well, to provide technically comprehensive help desk support and device maintenance.

Dr. Hemant Chaskar is the Vice President VP of Technology and Innovation at AirTight Networks, USA; he is responsible for AirTight's technology innovation, product strategy, and intellectual property management and protection. He has been in the technology and R&D industry specializing in security, wireless communications and networking for more than 12 years and has several granted and pending patents in the aforementioned technology areas. Prior to AirTight Networks, Dr Chaskar was a research principal at Nokia, where he led several corporate R&D programs in 3G/4G IP based mobile networks and also forged research collaborations with top universities. Dr Chaskar has published several research papers and has been an active contributor to the networking protocol standardization groups. He is a frequent speaker at technical conferences.

Hemant Chaskar holds a Ph.D.in Electrical and Computer Engineering from the University of Illinois at Urbana-Champaign, USA

BYOD (*bring-your-own-device*) tide is on the rise. Generally speaking, BYOD means freedom for the employees to use devices of their choice at the workplace. Fuelled by smartphone and tablet revolution, BYOD is expected to have profound impact on the workplace culture and the workplace management.

How BYOD impacts people depends on the roles they perform in their organizations. In general, employees and IT evangelists speak in favour of the BYOD trend, but workplace managers worry about the costs and risks of embracing this enterprise trend. A BYOD survey of over 300 IT and security professionals in North America, that we conducted in 2012, shows clearly that the enterprises understand that the BYOD trend will continue, but that they are at different stages of acceptance or understanding the benefits and challenges. There are a variety of issues enterprises will have to grapple with when planning their BYOD transition.

Trend, productivity, and cost savings

Current trends, productivity increases, and cost savings are the most commonly stated drivers behind enterprise BYOD adoption. Some studies have even shown that a strikingly high percentage of college students and almost equal percentage of employees said they would accept lower paying jobs in return for freedom to user their own device at workplace. Proliferation of smart phones and tablets has also built a personal bond between the users and the devices that they use. So companies are adopting BYOD to attract and keep the best talent. Letting the employees choose their own devices at work - those they are most comfortable with - might also result in productivity gains.

Companies have also been considering the cost savings that can result from BYOD. Cost savings can result when employees pay for their own devices in return for the freedom to use devices they prefer. Companies might also benefit by negotiating cheaper bundled services plans from their mobile operators. In practice, however, many companies will buy the devices the users prefer and, quite probably, pay for the services as well, so BYOD cost savings may or may not occur.

In our survey, network administrators were asked: How do you view the BYOD trend for your enterprise? Fully 61 per cent said they viewed it as both an opportunity to reduce IT costs and increase employee productivity.

Personal data, corporate policies, and legal aspects

BYOD is becoming popular and employees may want to use the same device both for personal and work matters. Some companies are in favour of sharing the same device for personal matters and work; they believe that the convenience of a single device will lead employees to carry it everywhere, which may make them even more productive. When we

asked IT executives about how pervasive they thought the use of personal smart devices was in their environment, 87 per cent said either 'very pervasive' or 'somewhat pervasive'. Other executives, though favour keeping work devices separate from personal devices; the believe that devices used at work should host corporate controls which can interfere with their personal data and privacy.

Whichever way, corporate policies need to address sharing and establish clearly defined policies regarding how to deal with personal data on devices used at work. For example, enterprises may install a remote wiping control on devices used at work; this will let them wipe out the data on it if the device is lost or stolen. The remote wiping may remove personal data in addition to the corporate data based upon how these data are stored on the device.

Difficulty can also arise in separating personal information from work information when legal matters such as the discovery are involved. Storing and accessing personal information on a work device might turn personal information into legally 'discoverable' information in the event of legal proceedings. Accordingly, companies must define concrete corporate policies regarding these matters and users will have to be aware of these policies, and formally accept these policies when BYOD is allowed.

Provisioning, help desk, and device maintenance

The BYOD devices that employees use will often have to be adapted by the IT department to enable the installation of enterprise applications. BYOD devices can be just about anything - smartphones, laptops, tablets, mini pads and who knows what - and each has its own OS environment. To service all these different devices, IT departments will have to develop the knowledge, skills and tools to deal with a very wide range of devices and operating systems.

BYOD also means help desk personnel will need the skill, knowledge and tools, including a very comprehensive technical knowledge base, to be able to resolve trouble tickets for such a diverse set of devices. The overhead for device maintain - as well as for software upgrades, patching and so on -increases in proportion to the diversity of the devices involved.

It is not reasonable to expect an IT department will have the knowledge and the tools to deal with all types of devices and platforms. In practice, then, BYOD is likely to be restricted to a limited set of devices and environments. Even so, this is a dramatic change from the way IT has worked in the past. IT departments have typically focused on standardising user devices for ease of management and to better service the users. With the BYOD, IT departments must manage a wide range of different devices and this will necessarily cost more to do.

Device security, data security, and network security

BYOD creates new information security challenges, especially with regard to corporate data and corporate networks. Corporate IT departments will have to work harder to ensure that employees' devices remain free from malware and viruses, to protect the devices themselves, and to avoid spreading problems to other corporate assets.

Some organisations might feel it necessary to restrict the applications that can be run on their emplyees' BYOD devices; they might even insist upon the use of a protected 'sandbox environment' to run corporate applications. Most companies will also install applications on BYOD equipment to protect corporate data in the event the device is lost or stolen.

In addition, some form of gate keeping is required at the corporate network's edge to monitor the devices that attempt to connect and to authorize only those devices that meet the security watermark.

When new employees enter an organisation, IT departments must be able to install whatever tools, software or hardware modification are needed to bring the employee's device up to an acceptable security threshold before the device becomes eligible to connect to the corporate network and data.

With BYOD, wireless will emerge as the primary medium for enterprise network access. As such, organisations will need to fortify their wireless security systems to avoid exposure to over the air attacks. Overall, significant investment is required to ensure that the BYOD adoption does not compromise information security.

Our survey found that 69 per cent of the respondents claimed that BYOD affects the measures they are taking for network security.

BYOD can enhance the workplace environment, increase productivity, and achieve cost savings. However, to reap these benefits, organisations have to carefully study the investment involved and the processes, policies, IT infrastructure and security needed to make it successful. BYOD, in some form, will spread to most companies in near future. So it is good time to start charting your own game plan for BYOD adoption.