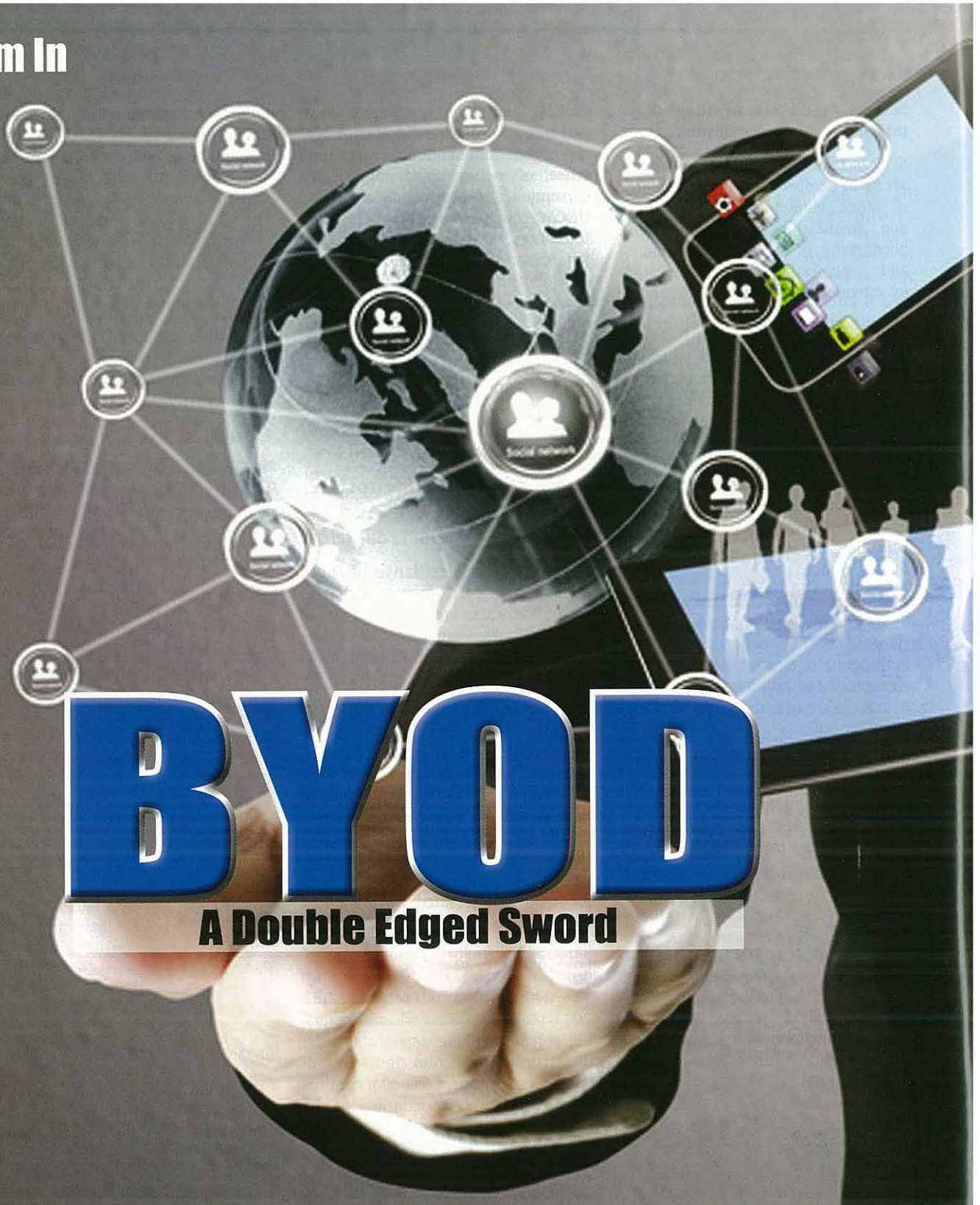
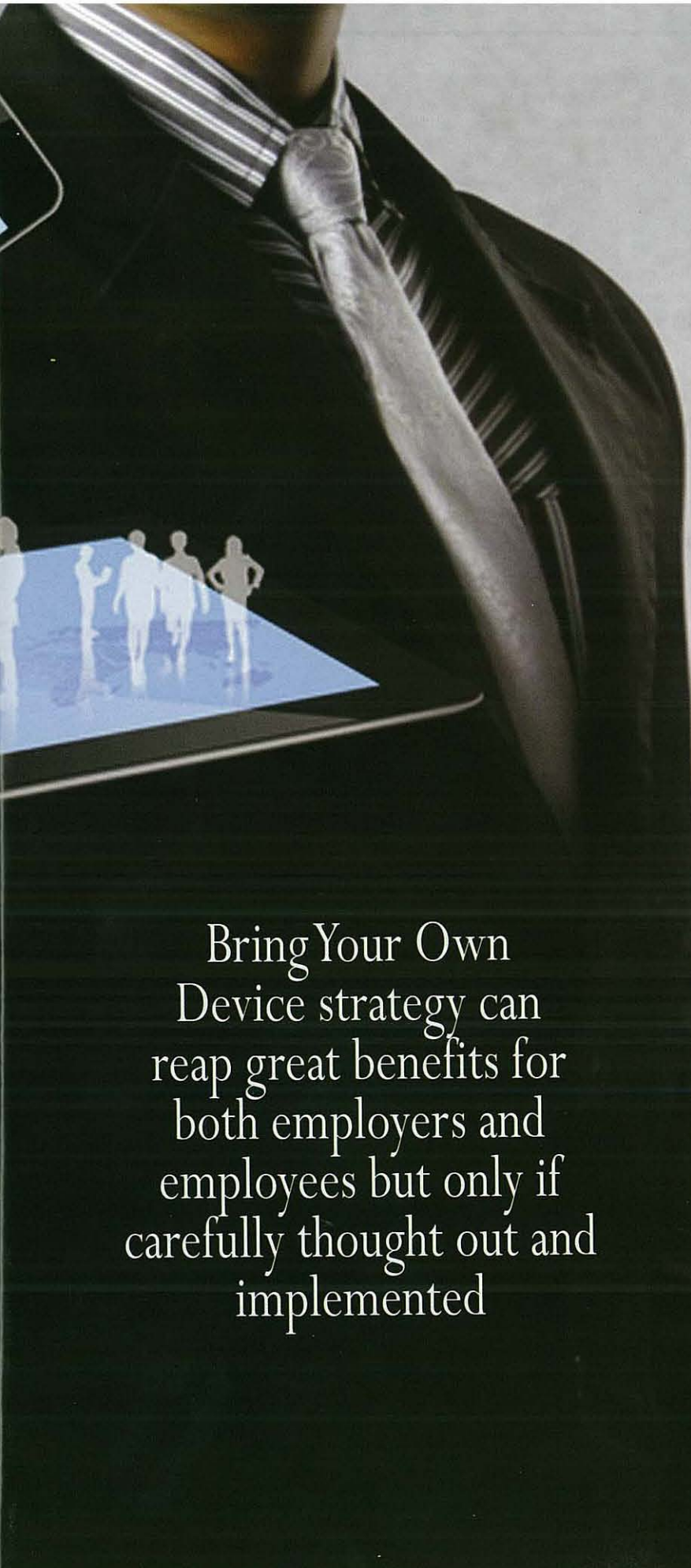


BYOD

A Double Edged Sword



Bring Your Own Device strategy can reap great benefits for both employers and employees but only if carefully thought out and implemented

Vivek Kathpalia
Partner
Nishith Desai Associates

Rakhi Jindal
Senior Associate
Nishith Desai Associates

The zeitgeist of our times appears to be consumerism and communication. In such times, it is hardly surprising that the "Bring Your Own Device" ("**BYOD**") movement is fast catching on. BYOD refers to the growing phenomenon that allows employees to literally bring their own devices to perform company work. These devices could range from blackberries, iPhones and a variety of android smart phones.

The Business Case for BYOD

Cost is definitely a factor that determines the adoption of any new mechanism by a company. But it would be simplistic to believe that cost would be the only factor that determines whether a company would adopt BYOD. There are a number

of trends as well as behavioural changes which have contributed to the growth of this phenomenon. Today, more than ever before, the boundaries between company time and personal time are increasingly getting blurred. Most employees are 'on call' in some way or the other (either fully or partially or minimally) when not in office premises. The rise of the smartphone and the resultant access to a wide variety of communication capabilities means that employees can access information and work from literally anywhere outside the office.

BYOD is here to stay; even if it means that this trend may evolve into as many different forms as there are business models today. So it may be more appropriate to ask how (instead of if) businesses are adopting this trend

Not so long ago, office computers would be better equipped to deal with business requirements. Today, network capabilities and computing power of most devices are such that there really is not much difference between office computers and personal devices in terms of ease of use.

Gone are the days when the Information Technology department would have stronghold over the technology to be used by the company and employees would be educated by the IT department on the use of gadgets and technology. Today, most employees are technologically savvy and have the spending power to purchase most if not all the devices and applications that they want to use. Indeed the consumerisation of information technology has become so widespread that it is often employee demands that determine the devices and applications that the company may purchase and utilise for its businesses.

In such a scenario, it is not surprising that a trend which gives employees power to decide the devices that they want to work on is fast catching on.

Businesses Adopting BYOD

According to a global study carried out by Gartner, 38% of companies expect to stop providing devices to workers by 2016[1]. In 2012, Cisco carried out a survey on BYOD and virtualization. The report is interesting in its findings that while the US is the global leader in BYOD adoption and policy, India along with US are the leaders in desktop virtualization[2].

BYOD is here to stay; even if it means that this trend may evolve into as many different forms as there are business models today. So it may be more appropriate to ask how (instead of if) businesses are adopting this trend. In some cases, businesses may adopt a staggered approach wherein BYOD is allowed or mandated for a select group of employees; mostly employees who need to be 'connected' constantly in 'real time'. In other cases, companies may offer an 'opt out' alternative for employees who do not want to use their personal devices.

Challenges in adopting BYOD

While BYOD no doubt provides various benefits to employees in terms of control and convenience as well as employers in terms of cost, there are a number of issues that companies need to consider while implementing BYOD or even while deciding not to implement BYOD.

Policy: Often the lack of clear policy around a corporate issue can lead to confusion amongst employees and possible liability for employers. Companies are discussing and should discuss the adoption of this trend. Companies should have clear BYOD policies which describe participation of the employees in the BYOD scheme, the level of control the employer is to have, whether the employer accepts some of the costs associated with the device, the expectation of privacy which employees may have. In some cases, the policy may be a negative policy that prohibits BYOD. The bottomline is that the company's stand should be made clear; this will not only make clear the behaviour that the company expects from its employees but it would also help the company to establish its case and bona fides should the need arise.

Control and Privacy Issues: One of the main issues in BYOD that may worry employers is the loss of control that would be faced if employees use their personal devices for company work. The level of control could vary depending on whether the device is wholly owned by the employee or partially paid for by the employee. If it is a personal device, then there could be reluctance on the part of the employees to have the employer dictate what activities can be performed on the device. For instance, if the company prohibits employees from accessing personal emails on a personal device, then it may be that the very purpose of the policy is lost. However, if reasonable restrictions are imposed such as blocking of certain social networking sites on company premises (which would be the case for company owned devices as well), then there is more likelihood of employee acceptance. Further, there may be

[1] "Bring Your Own Device: The Facts and the Future" cited from http://www.gartner.com/newsroom/id/2466615, [2] "BYOD: A global perspective; Cisco available at http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf [3] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 notified under the Information Technology Act 2000. [4] "VW to switch off BlackBerry servers outside work hours": The Telegraph, December 23, 2011 http://www.telegraph.co.uk/technology/blackberry/8974984/VW-to-switch-off-BlackBerry-servers-outside-work-hours.html. [5] For instance, The Factories Act, 1948 provides that where any worker works in a factory (involved in manufacturing) for more than 9 hours in any day or more than 48 hours in any week, such worker is entitled to overtime benefits.

reluctance on the part of the employee to have company security and monitoring methods and applications installed on the device. There may be claims of privacy violation by employees. Companies may need to consider whether to implement some sort of virtual divide between company information and personal information that reside in employee owned devices.

Another area which could result in major conflict is at the time of separation. Traditionally, employees leaving an organisation were expected to surrender all company devices and information. With BYOD, such a clear cut policy would not work. Employers need to be reasonably sure that their data and information is protected from intentional or even unintentional misuse in the hands of ex-employees. Similarly, employees need to be assured that ex-employers do not impose unreasonable control over their devices and data after separation.

India does not have very clear laws on privacy in such areas. However, India has been gearing up its machinery to deal with data protection issues and has implemented new laws for the protection of sensitive personal information[3]. Despite such developments, the fact is that Indian law in this area is nascent. In the absence of clear laws, company policy assumes great importance. The employer needs to be clear about how much control and monitoring is required and necessary for the employer. There has to be clear acceptance of employer led control and monitoring by the employees. If a company wants to adopt BYOD, it is imperative that a process be undertaken to obtain consent from all employees with respect to the BYOD policy adopted by the employer. For new recruits, this should ideally be part of the induction process.

Investigation: One area which is likely to give rise to issues which may be specially relevant to the legal community is that of investigations of employee-owned devices. Today, law enforcement agencies such as the police are well aware of the power of the personal phone and are equipped to conduct forensic audit of personal phones. Where such audit is initiated by law enforcement agencies, employees (or indeed anyone else) would most likely have to cooperate. But such audit may not be restricted to investigations initiated by law enforcement agencies; companies may also initiate internal investigations when there have been breaches of law or contractual obligations by employees such as breach of confidentiality. In such internal investigations, companies have to weigh in the possibility of employee resistance to the forensic audit of personal devices. Such audit processes and monitoring discussed above need to be handled with extreme care as it could lead to potential exposure.

Other Costs: While BYOD may ensure that the employer saves costs on the physical devices, does it mean that there are no overheads in terms of maintenance and trouble shooting. IT departments may find that there is added effort in maintaining and troubleshooting for a variety of employer devices. There may be issues where employers and employees disagree on what kind of and how much support should be provided to employee owned devices. Here too, a clearly defined company policy will help to minimise conflict.

Overtime: Companies seeking to implement BYOD may need to be wary of jurisdictions with strict working hour regulations. Various issues could arise when employees check email or perform other company work outside of office hours. It is true that such issues would exist even where employees use company owned devices, however it is likely that the issues would be heightened where the employees use personal devices. News reports indicate that in Volkswagen Germany, rules have been formulated under which emails will only be forwarded to company smartphones held by union workers (and not senior executives or other non-union workers) for 30 minutes before and after the actual working hours[4]. While India may not have such sophisticated laws, most Indian regulations which provide for overtime benefits are for the benefit or workmen and not managerial employees[5].

BYOD may open up a host of issues that employees and employers may face. Given these issues, it is important for companies to analyse how effective BYOD can be. If harnessed in a responsible and respectful manner, this phenomenon is likely to reap great benefits for both employers and employees. Mostly issues arise where companies adopt an ad hoc approach and deal with issues as they arise. If companies carefully think out, document, implement and maintain a robust BYOD policy, it would be possible to minimise a lot of issues or at least adopt an appropriate risk mitigation strategy.

If harnessed in a responsible and respectful manner, this phenomenon is likely to reap great benefits for both employers and employees. Mostly issues arise where companies adopt an ad hoc approach and deal with issues as they arise. If companies carefully think out, document, implement and maintain a robust BYOD policy, it would be possible to minimize a lot of issues or at least adopt an appropriate risk mitigation strategy

Disclaimer – The views expressed in this article are the personal views of the authors and are purely informative in nature.