BYOD in the UAE

by Sana Saleem

July – August 2012

In the consumerization of IT, bring your own device (BYOD) refers to the use of personal devices, such as smartphones, laptops and PDAs, for work purposes, including connectivity on the corporate network.

In the United Arab Emirates alone, consumers spend three times more than enterprises on IT – smartphone penetration in the UAE is 47%; higher than the US which stands at 40%. Employee productivity can be increased by making advantage of the popularity of mobile devices. Although cost savings can be realized by companies exploring this avenue there are IT issues that should making the switch.

BYOD: THINGS TO KEEP IN MIND

While an increase in employee satisfaction and productivity is a valid consideration, there are several challenges to implementing a BYOD policy:

Security

It is very dangerous for a device that is loaded with company data and emails to fall into the wrong hands. Most mobile devices come with basic security features like passwords and locks. However, many users do not enable these, and when they do they use very weak passwords. A device's inbuilt security features may not be entirely reliable. Companies planning on allowing BYOD must first educate their employees on best practices for securing their devices. The use of complex passwords and should be a consideration when giving corporate users access to business applications.

Smart phones come in many shapes, forms and operating systems. Companies should decide how much they can invest in making the proper modifications to connect each employee's personal device tothecorporatenetwork.Moreover,given the variety of IT issues users are likely to encounter, corporate users must also decide who is responsible for the device's technical support before considering a BYOD policy. If BYOD means that the IT team will have to be familiar with a range of devices, there will be a cost impact.

Malware/Viruses

The often indiscriminate use of personal smartphones, laptops and PDAs to access applications, documents and social networking sites can leave personal devices open to a variety of viruses and

malware. Corporate users are also more prone to targeted attacks using unique malware designed by hackers to gather sensitive information. Companies should put in place an acceptable usage policy in order to ensure that employees are not unwittingly disclosing sensitive corporate

information and documents when using personal devices on the company's network.

Before implementing a BYOD policy:

- Develop an accurate picture of the nature of the data and classify it in order to determine its sensitivity level.
- Determine where the corporate data is stored (i.e. which systems and devices it is stored in, and what back-up procedures anddisasterrecoverypoliciesareinplace).
- Review how and where employees, contractors and visitors to the company can access, copy, and transmit data.
- Institute a workable usage policy and code of conduct for how users should use their devices.
- Install security on all computers and mobile devices owned by the company, and work with employees to ensure that they have installed up-to-date security software on their devices.

SETTING UP AND ENFORCING A BYOD POLICY

Companies that allow or are considering allowing employees to use their own mobile devices at work should implement a BYOD security policy that clearly outlines the company's position and governance policy to help IT better manage these devices and ensure network security is not compromised by employees using their own devices at work.

Two departments that should be consulted regarding the development of a BYOD policy are the IT and HR departments. An IT department has the technical expertise to provide information on the abilities and limitations of devices and give insight on its capacity to support and handle logistic challenges presented by the use of a range of devices. Further, an IT department can provide information about the security of sensitive material on personal devices and provide guidance on the kinds of policies that would aid in data protection.

To ensure data security, companies should set up a secure remote access procedure that details the technical steps users must take to connect their devices securely to any company-connected network. Furthermore, a "digital certificate" (i.e. a means to verify that a user sending a message is who he or she claims to be) should be installed on every device so that e-mail and calendaring functions can be authenticated between the device and the company server.

The HR department is instrumental to the development of a new BYOD policy and must make sure that it integrates all existing policies without contradicting the same. It determines the penalties for not adhering to the policy and ensures that the policy and penalties are in line with company standards. Competent legal assistance should be sought to draft such policies and procedures to ensure that they are suited to the task.

Adapting to the changing technology landscape and industry demand is a routine exercise for all businesses but it is important to undertake such changes in an informed manner so as to avoid security risks and needless cost.

Al Tamimi & Company's Technology, Media & Telecommunications team, led by David Yates, regularly handles issues arising from the impact of technological developments in a business context.

Our Employment and Incentives team, led by Samir Kantaria, regularly advises on HR policies, and legal compliance in the context of employment relations. For further information about BYOD and its impact in an employment context, please contact David Yates (d.yates@tamimi.com) or Samir Kantaria (s.kantaria@tamimi.com)

The writer wishes to thank Ahsan Hasnani for his contribution to this article.