**Recruitment and the rise of BYOD**

BYOD stands for Bring Your Own Devices, and it is a policy which allows employees to bring and use their own mobile devices at their places of work. These devices include laptops, smartphones and tablets. Even though the devices are personally owned, BYOD facilitates their access to confidential company information, software and applications. Despite the fact that the concept has only been in implementation for a few years, it is a rising trend with businesses constantly coming up with innovative security plans in order to mitigate the risk that comes with the program.

For this reason, the recruitment process has also evolved to incorporate this demand. In the course of recruitment, the organization needs to be clear about their position on BYOD and consequently, communicate it clearly to applicants.

Merits of BYOD to Business

One of the main advantages of the BYOD policy for businesses is that the cost of hardware is shifted from the organization to the employee. This is in addition to voice services, data and other related expenses. Employees often do this without resistance because it is a personal investment.

Moreover, companies which implement BYOD, report higher satisfaction among their employees. By permitting them to use their own devices, they get to perform their tasks on devices they have chosen for themselves, and which are suited to their personalities and preferences. This is in direct contrast to being required to use a random device that has been chosen and issued by the organization, and to which the user has no attachment. The personal touch enables employees to feel more comfortable and invested in the company. Additionally, through BYOD, companies are able to benefit from the cutting edge features that employees incorporate into their devices in order to improve their performance.

Concerns regarding the BYOD policy for Businesses

Even with the trends generally leaning in favor of BYOD, there are a number of implications which the company needs to consider during the recruitment process. The main concern with BYOD is security. Through company-issued devices, it is relatively easy to monitor viruses and possible breaches into the company’s database. However, with BYOD, devices may be brought in with viruses and other malware which, once connected to the network at work, could damage the entire system. In addition, BYOD may cause the network and systems of the organization, more vulnerable to breaches. This is because a hacker would only need access to one device in order to potentially, connect to the company’s sensitive information.

However, with effective and consistent management, it is possible to safeguard against these risks. Employees are required to be vigilant about the security of their devices at all times, whether they are being used for work or not. Most organizations also require their staff to have antivirus software that is up-to-date and running. In addition, any anomalies with the devices may need to be reported in order to investigate possible vulnerabilities within the system. In order to eliminate the possibility of have sensitive company information leaked out or hacked into, it is recommended that staff members who deal with this kind of material not bring their own devices. These safeguards should be communicated during recruitment for companies which implement BYOD, as well as the consequences to the employee, if the security measures are not complied with 100 percent.