inspired
insights

inspire

Is the **'Cloud'** the answer to solving **BYOD** security **concerns?**

Some interesting statistics were published recently by Intel and readwrite.com about the growing prevalence of 'bring your own device' or BYOD culture within corporate industries. In April 2013, they recorded that 82 per cent of surveyed companies permitted some or all of their technically adept employees to use their personal IT and devices. This allowed the workforce to work more flexibly and efficiently, improving connectivity and reducing costs.

As cloud based infrastructure grows in popularity, driven by the availability of multiple online storage and backup services, increasingly whole workspaces are using it to promote connectivity and collaboration between employees. Of the employees surveyed by Intel and readwrite.com, 58 per cent believed their own satisfaction and productivity benefited from BYOD.

Security **Issues**

Employers have some concerns about compatibility with existing systems and regulatory issues; however security is at the top of the list when it comes to storing sensitive data outside the local work environment. In the IBSG Horizon Study, commissioned by Cisco Systems last year, company executives confirmed that protecting privacy and security were their top challenges. The key for businesses effectively revolves around choosing the right governance and support models, and implementing best security practice in relation to both device and endpoint, when developing cloud computing and BYOD policies.

This means a multifaceted, bottom-up approach to security is needed. The vulnerability of data stored outside the workplace needs to be recognised and understood by company executives and chief information officers, who may not always appreciate the threats and liabilities involved when embracing cloud technologies. Data stored in the cloud is only as secure as the protective measures that a company puts in place to prevent unauthorised access.

Endpoint Security

Increasingly, employees are able to access large quantities of sensitive data, which can be downloaded and stored in personal laptop and mobile devices. It is not enough for companies merely to protect the data stored in the cloud, they must also consider the security of the source, the localised endpoints and every device and touch point between the source and the cloud.

Desktop virtualisation provides a different way of working that helps make devices more secure, at least as far as company information is concerned. Employees can log in to their desktop environment, which is high-powered and fully functioning, from a wide range of locations and devices using their broadband connection but no data is stored locally on their device. Security of their device is thus no longer an issue and with a virtual OS, multiple staff members' desktops can be hosted on one server. This solution offers more flexibility to the employee and reduces the cost to the employer.

When companies are developing new cloud and BYOD policies, priority needs to be given to confidentiality and security in order to achieve best practice. A report by Citrix Systems last year revealed that, while 92 per cent of businesses surveyed were allowing employees to bring in personal devices to the workplace, only 44 per cent had a formal plan in place relating to BYOD and to managing the use of personal technology.