BIZCOMMUNITY

Leveraging the advantages of BYOD

By Gareth Tudor

19 Jun 2014

The Bring Your Own Device (BYOD) trend, which has employees making use of their own smartphones, tablets and notebooks for business purposes, is a growing phenomenon in the business world. This is especially so in the light of the fact that a recent estimate has the average employee using up to five devices.

BYOD has many advantages to offer organisations of all sizes, including improved productivity and efficiency. However, it also introduces a significant challenge - allowing multitudes of devices onto a corporate network. These devices are, moreover, not under the organisation's direct control and can open up security risks, particularly with regard to sensitive corporate data. Comprehensive data protection, including end-point data encryption, cloud-based back-up and recovery, and effective policies, are critical in ensuring that organisations can maximise the benefits of BYOD while minimising the risks.

Mobility is one of the most disruptive innovations in the business world over the past few years and, as technology evolves, more and more people are taking advantage of the ability to work on the road, on the move and from any location. BYOD is one of the biggest drivers of mobility and many organisations are looking to implement a BYOD strategy for employees. However, security remains the number-one challenge and risk factor for organisations looking to allow BYOD.

Whenever a device is connected to the organisation's network, systems, or computers, the potential exists for exposure to viruses and malware, not to mention hacking. In addition, intentional or accidental copying of sensitive information to unauthorised devices can occur. Furthermore, due to these devices being mobile by nature, they are prone to loss or theft, which hugely increases the risk of data being vulnerable. With the well-known consequences of compromised data, and the impending enactment of the Protection of Personal Information (PoPI) Act, protecting sensitive information is more important than ever. As such, there are a number of considerations that should be taken into account to ensure that BYOD is securely implemented.

Develop effective BYOD policies

The first step is to develop effective BYOD policies to govern the use of devices in the organisation. Policies need to apply to all employees in an organisation, including part-time staff, consultants, temporary employees and contractors, and must outline the steps necessary for ensuring security when users' personal devices are connected to an organisation's systems. Policies should cover all commonly used devices, including desktops, laptops, tablets and smartphones, as well as flash drives, memory sticks and external hard drives. A BYOD authorisation process should also be outlined, applicable whenever an employee wishes to use a personally owned or personally provided device to connect to an organisation's network.

Once policies are in place, it is critical to ensure protection of data belonging to the business and residing on these highly mobile devices that are often outside of the control of the organisation. This requires a twofold approach - protecting the data on the device from falling into the wrong hands, and ensuring that adequate back-up and recovery systems are in place.

Comprehensive data protection on mobile devices requires a solution that will address data security at the source - on the device itself, with encryption and security tools to deliver data protection, access control and rights management. On-device data encryption and security can help to prevent data on mobile devices from being accessed by unauthorised parties, in case the device is lost or stolen. Rights management and access control ensure that only permitted users can view data, and policies can be set as to which data must be encrypted, so that corporate and personal data can be separated, which is vital in the BYOD scenario. To enhance security further, on-device encryption can be linked into cloud-based back-up and restore solutions, the second vital aspect of data protection for BYOD.

Cloud-based back-up and restore is essential for mobile devices, as they are not always connected to corporate networks and servers. Solutions should enable scheduled, involuntary back-ups, regardless of the secure network the user is connected to, in order to ensure compliance. Back-up also needs to optimise bandwidth usage to minimise the effect on the user's experience and incorporate mid-file restart capabilities, to allow back-ups to continue in the event of interruptions without the need to restart the entire process. Back-up policies should cover all authorised BYOD devices to ensure that data is always protected, no matter where the user is working or what device he has.

Implementing an effective BYOD strategy that ensures that organisations can leverage the benefits without exposure to unnecessary risk requires a multi-fold approach to data protection. Ensuring this is done correctly is essential, as the consequences of getting it wrong could be detrimental to the business. Partnering an experienced service provider, which can help organisations to develop effective and inclusive best-practice BYOD policies and suggest solutions for the protection, encryption and back-up of data, can help organisations remove this complexity. Ultimately, BYOD will only continue to grow and organisations need to ensure they are protected in order to take advantage of this trend.

ABOUT GARETH TUDOR

Gareth Tudor is the CEO at Altonet, an ISP and provider/integrator of backup and restore solutions. Tudor started his career in finance after he qualified as a chartered accountant (SA) and has subsequently garnered a wealth of experience in a number of businesses, including his own.

- Metadata - playing a vital role in back-up and recovery - 3 Sep 2014
- How secure is your critical data in the cloud? - 18 Aug 2014
- Leveraging the advantages of BYOD - 19 Jun 2014
- Avoiding the consequences of data loss - 29 Aug 2013

View my profile and articles...