

BYOD: What are the security concerns?

By Andre Edmond
Sr. Security Engineer

According to Wikipedia

The term BYOD (Bring Your Own Device) first entered common use in 2009, courtesy of Intel when it recognized an increasing tendency among its employees to bring their own devices (i.e., smartphones, tablets and laptop computers) to work and connect them to the corporate network. However, it took until early 2011 before the term achieved any real prominence when IT services provider Unisys and software vendor Citrix Systems started to share their perceptions of this emergent trend.

Problems with BYOD

- Malware and other attacks if the device is not used in a secured manner (X-rated sites or downloads of unsafe applications).
- Lost or stolen devices: Company data can be at risk especially if the device is not secured with a strong password or passcodes.
- Staff turnover: If someone quits without any notice you won't have time to wipe the device of its information.
- Transfer of company data over unsecure connections
- Company data and personal data comingling.

Benefits of a BYOD Policy

- Increase employee productivity and efficiency
 - Employee can readily access company information to do their job using their personal devices from within the company or remote locations.
- Increase worker's satisfaction
 - Due to the convenience.
- Saves the organization money
 - Eliminates the need to buy equipment and devices for each employees.
- Reduce amount of training
 - No need to train employees on how to use the device.
- Up-to-date Devices
 - Most employees have the latest technology.

Mitigating Controls

- Have a BYOD policy that clearly states what will be supported, security measures, acceptable usage agreement, what type of data they can access etc.
- Cyber Liability Insurance coverage for the risk associated with BYOD. It should clearly define who is responsible for stolen data or a data breach as the devices are being used outside of the workplace environment.
- Use mobile device management technologies to enforce protection on employees' mobile devices.
- Provide staff instructions on maintaining security when using their mobile devices.

Thank you!

For More Information Contact:

Andre.Edmond@LexisNexisRisk.com

Or on LinkedIn at:

<https://www.linkedin.com/in/andre-edmond-166129b4/>