HE Update

Is it ok to use personal technology at work? Bring Your Own Device (BYOD) in HE

February 2015

Background

For many people, work happens at any location, any time and with whatever electronic device is handy. The trend for staff to use their own devices for work is known as BYOD. In practice this can mean checking work email on a laptop in the morning, reviewing documents on a mobile phone on the train, or editing presentations on a tablet while watching TV. However it happens, university data is outside the network and potentially unprotected. More and more of us take BYOD for granted and it's increasingly a routine expectation for staff to be able to avail of this option.

Last year Uniac completed a BYOD benchmarking exercise which found that:

- Universities were allowing the use of BYOD, however the majority had no usage policy
- The majority offered some basic IT support for BYOD
- BYOD costs i.e. insurance; applications etc. were not generally reimbursed by the Universities
- The majority did not have a policy covering the use of cloud based services
- No institutions were aware of any security breaches regarding cloud services and BYOD.

Since then, it's fair to say we've seen the trend towards BYOD continue at an incredible pace. We're now seeing increasing demand for BYOD in all areas and institutions are asking themselves: **What are the risks and are the risks manageable?**

This briefing sets out some of the risks facing HE organisations and will help guide institutions in managing those risks.

BYOD Risks

- University data may be copied to insecure devices which can be easily hacked and have data stolen
- Insecure personal devices may be lost, leading to loss of corporate data
- Personal devices may be shared, leading to unauthorised access to University data
- Data on personal devices won't be visible to the organisation, making it difficult to manage
- Data stored on multiple devices can create chaos with version control and record keeping
- People may not delete University data stored on their personal devices when it's no longer needed

- Data is often transferred insecurely via email to personal devices.

So in summary the security of data may be compromised; day to day business can be made more difficult and Data Protection and Freedom of Information compliance made more difficult – if not impossible to achieve.

What should HE institutions be doing?

The other side of the argument is that many university staff experience improvements in productivity and collaboration through use of their personal devices and we feel that it is important to support this way of working, just as long as the right digital security is in place to protect the University.

Policy & Education Actions:

- Insist on a base level of security such as passwords on devices
- Develop policies on BYOD acceptable use and cloud storage
- Outline consequences for staff who do not adhere to the policies
- Educate BYOD users of the risks surrounding public Wi-Fi networks so that they can make an informed decision when selecting a Wi-Fi network.

Technical solutions:

- Deploy corporate endpoint protection to personal devices. End to End encryption protects data when using unsecure Wi-Fi
- Protect sensitive data with appropriate network segmentation and access controls
- Deploy continuous vulnerability scanning
- Record detailed log information for system/data access and changes. Develop event alerts and analyse the logs.

So to answer the original question – 'Is it ok to use personal devices at work?' - we think the answer is to take a risk based approach which means that for most areas, the answer is yes, as long as the right controls are in place and operating effectively. However, this is a complex area with many different variables and the right solution must be developed with consideration of the individual circumstances and risk profile of the institution concerned.

How can we help?

The Uniac IT Audit team has an extensive and proven track record in providing assurance and consultancy services to help the HE sector manage IT risks and we can:

- Provide independent assurance on the effectiveness of risk management relating to BYOD
- Give insight into the current position of the organisation
- Identify weaknesses that expose the organisation to risks
- Make recommendations to help institutions to manage their BYOD risks.

To discuss any of the issues raised in this briefing note, or to find out how Uniac can assist you in managing BYOD risks, please contact the Uniac specialists in this area:

Key Contacts

Robert Foster
IT Senior Auditor
rfoster@uniac.co.uk
0161 247 2851

Ian Musgrave
Head of IT Audit
imusgrave@uniac.co.uk
0161 247 4697