UPDATED FEBRUARY 2014

Bring Your Own Device (BYOD) for Executives

Summary/Introduction

Bring Your Own Device (BYOD) scenarios enable organisations to take advantage of new technology faster. They also have the potential to reduce hardware costs and improve organisational productivity and flexibility.

However BYOD also introduces new risks to an organisation's business and the security of its information, which need to be carefully considered before implementation. This document summarises key BYOD considerations and risk minimisation strategies for Chief Information Officers and other senior decision makers.

Initial Considerations

1. **What are the legal implications?** Legislation such as the *Privacy Act 1988, Archives Act 1983* and *Freedom of Information Act 1982* can affect whether an organisation is able to implement BYOD in their environment and, if so, what controls need to be implemented to ensure all legal obligations can be fulfilled. BYOD can increase liability risk to an organisation. Organisations will need to be ready to manage issues such as software licencing, inadvertent damage to an employee's personal data, or expectations of privacy in the event of an investigation, Freedom of Information requests or incident response.

2. **What are the financial implications?** Organisations implementing BYOD may benefit from reduced hardware costs should employees pay for their own devices. However, there can often be an overall cost increase as a result of the need to technically support a variety of devices, manage security breaches or cover some costs associated with the employee's device.

3. **What are the security implications?** Devices storing unprotected sensitive data could be lost or stolen. Employees use corporately unapproved applications and cloud services to handle sensitive data. An organisation also has reduced assurance in the integrity and security posture of devices that are not corporately managed. Employees will often lack the IT knowledge and motivation to reduce security risks to their devices.

Approaches

4. The main security risk considerations in enterprise mobility, including BYOD, can be summarised in the four 'P's of enterprise mobility – **purpose, planning, policy** and **polish**.

5. **PURPOSE – take a risk management approach to implementing enterprise mobility.** A change in work practices will mean a change in risk profile. Organisations should use a risk management process to balance the benefits of BYOD with associated business and security risks. Determine whether there is a justifiable business case to allow the use of employee-owned devices to access and distribute their information.

6. **PLANNING – consider the different options available and make an informed decision.** Ask which users in your organisation require enterprise mobility either via the use of agency-owned devices or personally owned devices. What information do your users need access to, and how will they access it?

7. **POLICY – develop and communicate a sound usage policy.** This should be based on the risk assessment and business case and clearly communicate expected behaviour from employees. Establish what financial and technical support employees can expect to receive. Be consultative in your approach – the most effective scenarios are jointly developed by business and legal representatives, IT security staff, system administrators and employees themselves. This helps your organisation develop a realistic policy and processes which all stakeholders are willing to adhere to.

8. **POLISH – review your usage policies and monitor the enterprise mobility scheme.** You need to have regular reporting to senior management to help them understand and address unacceptable risks.

9. **Contact your IT Security Team.** In particular, seek answers to the following questions:

   a. *How do we protect our sensitive or classified information from unauthorised access?* For example, does your organisation keep sensitive or classified information in a data centre instead of on an employee's device (e.g. through use of a remote virtual desktop)?

   b. *How do we protect information on our corporate network?* For example, does your organisation limit and audit the use of BYOD on the corporate network? Is multi-factor authentication used for remote access?

   c. *How do we protect the device and associated network from malicious software?* For example, is the employee's personal operating environment separated from the work environment on the device (e.g. through use of a managed container)? Does your organisation require security patching, and limit privileges and access to corporate information from BYOD?

   d. *How do we reduce the risk caused by lost or stolen devices?* For example, does your organisation have the technical and legal ability, and user agreement, to remotely locate or wipe a device? Are employees required to regularly backup work data from their device to agency-sanctioned backup servers?

Further Information

10. Detailed guidance can be found in ASD's *Protect* publication *Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD).* This publication is available at www.asd.gov.au.

11. This document complements the advice contained in the *Australian Government Information Security Manual* and ASD device-specific hardening guides, available at www.asd.gov.au.

Contact details

Australian government customers with questions regarding this advice should contact the ASD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or asd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.