Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Bring Your Own Device for Executives

JANUARY 2019

Introduction

Bring Your Own Device (BYOD) scenarios enable organisations to take advantage of new technologies faster. It also has 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.

Initial considerations

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.

As 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 request or incident response activity.

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 support a variety of employee devices, manage security breaches or cover some costs associated with an employee's device or its use.

What are the security implications?

There are a number of security implications associated with BYOD. For example, employee devices storing unprotected corporate information could be lost or stolen, or employees could use unapproved applications and cloud services to handle or store corporate information.

Organisation are also likely to have reduced assurance in the integrity and security posture of devices that are not corporately managed as employees will often lack the knowledge and motivation to reduce risks associated with their devices.

Implementation approach

The main considerations in implementing enterprise mobility, including BYOD, can be summarised as: purpose, planning, policy and polish.

Purpose

Take a risk management approach to implementing enterprise mobility. A change in work practices will mean a change in risk profile. 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 devices to access and distribute corporate information.

Planning

Consider the different options available and make an informed decision. Ask which employees in your organisation require enterprise mobility either via the use of organisation-owned devices or personally-owned devices. What corporate information do your employees need access to and how will they access it?

Policy

Develop and communicate a sound usage policy. This should be based on a risk assessment 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, security staff, system administrators and employees themselves. This will help your organisation develop a realistic policy and processes which all stakeholders are willing to adhere to.

Polish

Review your usage policies and monitor your enterprise mobility implementation. Regular reporting to senior executives will help them understand and address unacceptable risks.

Contact your security team. In particular, seek answers to the following questions:

- How do we protect our corporate information from unauthorised access? Do we keep corporate information in a data centre instead of on employee devices?
- How do we protect corporate information on our network? Do we limit and audit the use of employee devices on the corporate network? Is multi-factor authentication used for remote access?
- How do we protect our networks from malicious software? Is an employee's personal operating environment separated from the work environment on their devices (e.g. through use of a managed container)? Does our organisation require security patching, and limit privileges and access to corporate information from employee devices?
- How do we reduce the risk caused by lost or stolen employee devices? For example, do we have the technical and legal ability, and employee agreement, to remotely locate or wipe their devices? Are employees required to regularly backup work data from their devices to organisation-sanctioned backup servers?

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.

Additional guidance on enterprise mobility and BYOD is available in the ***Risk Management of Enterprise Mobility Including Bring Your Own Device*** publication at https://www.acsc.gov.au/publications/protect/Enterprise_Mobility_BYOD.pdf.

Contact details

Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).