



Bring Your Own Device for executives

First published: November 2012
Last updated: October 2021

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 cybersecurity 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.

Organisations 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 [Information security manual](#) is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the [Strategies to mitigate cybersecurity incidents](#), along with its [Essential Eight](#), complements this framework.

Further information on enterprise mobility and BYOD is available in the [Risk management of enterprise mobility \(including Bring Your Own Device\)](#) publication.

Contact details

If you have any questions regarding this guidance you can [write to us](#) or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2021.

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)



Australian Government

Australian Signals Directorate