GOV.UK

Guidance

BYOD Guidance: Executive Summary

Published

Contents

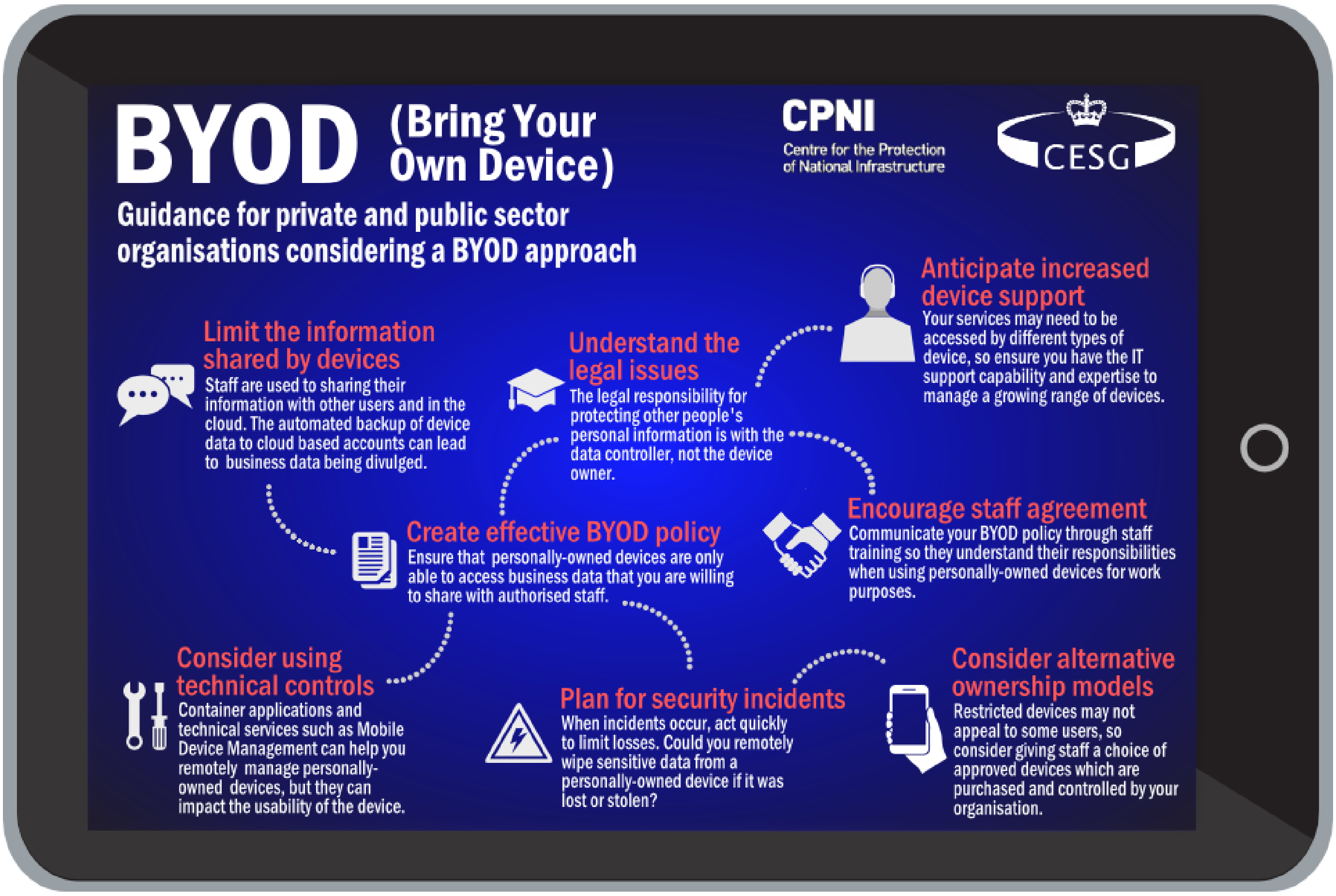
1. Introduction

With the rapid increase in the use of mobile devices and the growth of remote and flexible working staff now expect to use their own laptops, phones and tablets to conduct business. This guidance is for organisations considering a 'Bring Your Own Device' (BYOD) approach, and describes the key security aspects to consider in order to maximise the business benefits of BYOD whilst minimising the risks. It also provides a useful reminder for those already implementing a BYOD approach. It should be used to inform risk management decisions for BYOD deployments, and is particularly relevant for public sector organisations operating at OFFICIAL within such deployments.

- For security advice relating to specific mobile platforms, please consult the End User Devices Security Guidance.
- For information on security best practice for a range of mobile devices, please consult CPNI's Mobile Device Documentation.

2. BYOD at a glance

The key security aspects to consider are summarised in the following diagram, with each aspect described below.



BYOD (Bring Your Own Device)

Guidance for private and public sector organisations considering a BYOD approach

CPNI Centre for the Protection of National Infrastructure

CESG

Limit the information shared by devices
Staff are used to sharing their information with other users and in the cloud. The automated backup of device data to cloud based accounts can lead to business data being divulged.

Understand the legal issues
The legal responsibility for protecting other people's personal information is with the data controller, not the device owner.

Anticipate increased device support
Your services may need to be accessed by different types of device, so ensure you have the IT support capability and expertise to manage a growing range of devices.

Create effective BYOD policy
Ensure that personally-owned devices are only able to access business data that you are willing to share with authorised staff.

Encourage staff agreement
Communicate your BYOD policy through staff training so they understand their responsibilities when using personally-owned devices for work purposes.

Consider using technical controls
Container applications and technical services such as Mobile Device Management can help you remotely manage personally-owned devices, but they can impact the usability of the device.

Plan for security incidents
When incidents occur, act quickly to limit losses. Could you remotely wipe sensitive data from a personally-owned device if it was lost or stolen?

Consider alternative ownership models
Restricted devices may not appeal to some users, so consider giving staff a choice of approved devices which are purchased and controlled by your organisation.

BYOD infographic

3. Understand the legal issues

The legal responsibility for protecting personal information is with the data controller, not the device owner. The Information Commissioner’s Office (ICO) can impose fines of up to £500,000 for serious data breaches.

Read the ICO’s BYOD Guidance, and be aware of laws relating to your business data, in particular:

- the Data Protection Act (DPA), which states employees must take measures against unauthorised or unlawful processing of personal data
- the Employment Practices Code, which states that employees are entitled to a degree of privacy in the work environment

In addition, understand how your organisation’s obligations under the following acts can be met if staff are allowed to access business information and systems from personally owned devices:

- Regulation of Investigatory Powers Act
- Computer Misuse Act
- Freedom of Information Act
- Official Secrets Act

3.1 Impact on commercial agreements

You will also need to consider how any commercial or second party agreements are affected by adopting BYOD. For example, there may be existing commercial agreements between organisations that restrict the running of business software on personally owned devices.

4. Create effective BYOD policy

Think carefully about what business information and services you want staff to access using their own devices. If required, refer to the Architectural Approaches section of this guidance. You should design your network architecture so that staff can only access the information that you are willing to share.

Start by:

- preventing any unauthorised devices from accessing sensitive business or personal information
- ensuring that authorised devices are only able to access the data and services you are willing to share with BYOD employees

Use these requirements to form your organisational policy for BYOD, which you should document to clarify organisation and employee responsibilities. You may want staff to sign this to show they acknowledge and understand their obligations.

4.1 Bad policy undermines the approach and increases the risk

Polices that are too restrictive, in that they impact on the usability of the device, will drive down adoption and so undermine the approach. Such policies may encourage staff to find workarounds which increases security risk. A BYOD implementation requires new policy to cover the specific aspects of the BYOD approach, and changes to existing policy if your organisation is to fulfil its corporate and legal obligations.

5. Limit the information shared by devices

One of the advantages of BYOD adoption is that personally owned devices are ‘always connected’. However this does have associated risks.

5.1 Understand how devices and users share information

Personally owned devices are designed to facilitate the easy (and often automatic) sharing of data, and device owners are used to sharing personal information with other users and in the cloud. BYOD policy should highlight the risks of sharing business data with unauthorised users. Consider how security problems in personal applications (eg blogs, social media) may affect your organisation’s applications, information, and network services. For example, users may inadvertently send social networking posts from their corporate identity instead of their personal account if both are configured on the device.

5.2 Automated backups

Some devices automatically store a backup of the data on a device to a cloud-based account, or to the user’s

PC. This is a risk that needs to be managed.

6. Encourage staff agreement

Communicate your BYOD policy through employee training and education. Ensure that your staff understand their responsibilities when using their own devices for business purposes. This is important because many employees' approach to security will differ when using their own devices compared to using a corporately owned laptop or PC. For example, staff may be happy to let family members use their own device, or provide credentials (including passwords) to a third party for maintenance or repair.

Conduct regular audits of the business data stored on devices; technical solutions can help with this. When staff leave your organisation or replace their device, ensure all business data is removed and access to business systems is revoked.

7. Consider using technical controls

There are a range of technical services, such as Mobile Device Management (MDM), that can help you remotely secure, manage and support personally owned devices.

Container applications, where data is contained within a specific application, can help to manage information flows between personal and business areas of a device.

However, these technical solutions still depend on the integrity of the underlying device and can affect its usability. It is important to balance technical controls with usability; if a solution is too restrictive, then staff may find workarounds or use unsafe alternatives to achieve their business goals.

7.1 Protecting against data loss

Where possible, provide staff with a 'presentation' of information on their device, rather than storing it locally. This minimises the data that can be easily accessed if the device is lost or stolen. Be aware that security solutions, such as encryption or container products, can be circumvented if malware is present on the device.

7.2 Implement effective authentication

Staff should be made to authenticate themselves before being given access to business data. Since personally owned devices are more likely to be infected by malware, some authentication credentials could be compromised. You should consider using different credentials for BYOD access to business systems from those devices which are given broader access. For example, usernames and passwords should not be shared between personally owned devices and the business desktop environment.

8. Anticipate increased device support

A successful BYOD approach could lead to services being accessed by different types of device. Implementation of any of the security controls previously applied to corporately owned devices may now need to be applied to a variety of hardware and software combinations. This will increase your support demand in terms of:

- the need to support a greater number of device types
- keeping multiple operating systems patched and up to date
- responding to security incidents across a variety of devices and operating systems

As your BYOD implementation expands, ensure you have sufficient IT support capability and expertise to manage a growing range of devices and device platforms. The associated cost of supporting a variety of devices, operating systems and user devices which will probably change quite rapidly in response to technical advances or user preferences should also be considered.

9. Plan for security incidents

Personally owned devices are lost, stolen and compromised every day. Should one of these events happen, it is important to have confidence that business data is protected.

When an incident occurs you should:

- act immediately to limit losses
- prevent the spread of any compromise
- learn lessons from the incident

Plan for and rehearse incidents where a personally owned device that has access to sensitive business information is lost, stolen or compromised. Ensure you are able to revoke access to business information and services quickly, and understand how you will deal with any data remaining on the device. Consider using a remote wipe feature for business data.

In addition:

- identify who in your organisation is responsible for replacing lost or stolen personally owned devices
- consider the effect any delay in the replacement of devices will have on your organisation’s productivity
- ensure that staff know who to contact and what to do if a device is stolen; staff must feel confident that they can quickly report incidents without fear of recriminations, especially if it’s their own device

10. Consider alternative ownership models

The less management control an organisation has on a device, the less confident it can be that data on it will be secure. Management controls can include the ability to control what software and data goes onto the device, how it is configured, as well as the ability to wipe the device remotely.

10.1 ‘Choose your own device’

For many users, surrendering control of their own devices would be unacceptable. Consider alternative ownership models, such as ‘choose your own device’, where staff are allowed to choose from a selection of approved devices which are purchased and controlled by the organisation.

10.2 ‘Corporately owned, personally enabled’

Alternatively, consider introducing a policy that allows staff to use corporately owned devices for personal tasks. These can include web browsing, media playback, and access to an approved set of applications available from the platform’s public application store. Organisations using this model should be aware of the risk of business data being shared via personal applications, and exposing the business to attack from compromised personal applications.

11. Further information

For further information on securing mobile devices for BYOD, visit the following resources:

- www.getsafeonline.org
- Information Commissioner’s Office
- CPNI Mobile Device Guidance

Legal information

CESG: This guidance is issued by CESG, the UK's National Technical Authority on Information Assurance. One of the roles of CESG is to provide advice to UK government entities and organisations providing services to UK government. The guidance found here is provided and intended for use by this audience. It is provided 'as-is' as an example of how specific requirements could be met. It should be used to help inform risk management decisions on the use of the products described, but it should not be used for procurement decisions; it is not intended to be exhaustive, it does not act as an endorsement of any particular product or technology, and it is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take appropriate technical and legal advice in using this and other guidance published by CESG. This guidance is provided without any warranty of any kind, whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, content, quality, or fitness for purpose of all or any part of it. CESG cannot, then, accept any liability whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it. This guidance is UK Crown Copyright. All Rights Reserved.

CPNI: Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.