National Cyber Security Centre

General Security Advisory

GSA-005-17

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

Bring Your Own Device (BYOD)

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 document outlines the key security considerations to maximize the business benefits of BYOD whilst minimising the risks.

What is BYOD?

BYOD policies have gained prominence as organisations look to take advantage of increasing enterprise mobility. Enterprise mobility can create opportunities for organisations to improve customer service delivery, business efficiency and productivity. Additionally, employees obtain increased flexibility to perform work regardless of their physical location.

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 CIOs and other senior decision-makers.

Initial considerations

Legal implications

Legislation, such as the Privacy Act 1993, 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, Official Information Act request or incident response.

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.

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.

How should we approach implementing a BYOD policy?

The Australian Signals Directorate has summarised the main security risks with the four 'P's of enterprise mobility:

- **Purpose** - take a risk management approach to implementing enterprise mobility. 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 company information.
- **Planning** - consider the different options available and make an informed decision. Which users require enterprise mobility either via agency-owned or personally-owned devices? What information do these users need access to and how will they access it?
- **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. The most effective scenarios are jointly developed by business and legal representatives, IT security staff, system administrators and the employees themselves. This helps ensure your organisation develops a realistic policy and process which all stakeholders ae willing to adhere to.
- **Polish** - review your usage polices and monitor your BYOD scheme.

Additionally, they recommend contacting your IT Security Team to seek answers to the following questions:

- *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)?
- *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?
- *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?

- *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:

Section 21.4 of the NZISM covers BYOD: https://www.gcsb.govt.nz/assets/GCSB-NZISM/NZISM-Part-Two-v2.6-July-2017.pdf

Review the ASD's BYOD Considerations for Executives at: http://www.asd.gov.au/publications/protect/byod_considerations_for_execs.htm or The UK NCSC's Executive Summary on BYOD at: https://www.ncsc.gov.uk/guidance/byod-executive-summary.

*The NCSC can be contacted by email via **info@ncsc.govt.nz** or by phone on: **04 498 7654**. We encourage you to contact us at any time if you require any further assistance or advice.*