Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

NOVEMBER 2012

Bring Your Own Device (BYOD) Considerations for Executives

Introduction

1. The popularity of Bring Your Own Device (BYOD) scenarios is increasing as a result of more consumers owning powerful mobile devices, such as smartphones, tablets and laptops, which can provide greater freedom, convenience and job satisfaction to employees. BYOD enables organisations to take advantage of new technology faster, and has the potential to reduce hardware costs and improve organisational productivity and flexibility.

2. However, BYOD will introduce new risks, both to an organisation's business and the security of its information, which need to be carefully considered before implementation. Importantly, there will always be residual risk in a BYOD scenario. This document summarises key BYOD considerations and risk minimisation strategies for Chief Information Officers and other senior decision makers.

Key Considerations

3. **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 request or incident response.

4. **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.

5. **What are the security implications?** BYOD can be the 'weak link' into a network. Using mobile devices for both personal and business purposes can create more opportunities for social engineering and the inadvertent installation of malicious software. Malicious software can provide an entry route into the associated corporate network and access to information communicated or stored on the device. Organisations are likely to have less visibility and control over the security configuration of, and user behaviour on, BYOD. Employees will often lack the IT knowledge and motivation to reduce security risks to their devices.

6. As users control the underlying operating system in a BYOD scenario, it is difficult to guarantee that a device can be trusted to connect to a corporate network. Although implementing DSD guidance can help improve the security of BYOD, it cannot mitigate all security risks relating to their use.

7. **Do I have a strong business case to justify the security trade-off?** An organisation will be making a security trade-off by allowing employee-owned devices to access and distribute its information. Ensure there is a justifiable business case to support the acceptance of residual security risk in BYOD scenarios.

Minimising Risk to Your Agency

8. **Take a risk management approach to BYOD implementation.** 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, as well as to determine whether there is a justifiable business case to allow the use of employee-owned devices to access and distribute their information.

9. **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 and permitted uses of BYOD, as well as what financial and technical support employees can expect to receive.

10. **Be consultative.** The most effective scenarios are jointly developed by business and legal representatives, IT security staff, system administrators and employees themselves. This helps ensure your organisation develops policy and processes which all stakeholders are willing to adhere to.

11. **Educate your users.** Ensure users are made aware of the corporate policy and organisational requirements, as well as actions they can take to minimise the risks of device compromise or loss.

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

   a. *How do we protect our sensitive or classified information from being stored on the device?* For example, does your organisation keep sensitive or classified information in your organisation's 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 logically 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 created on their device to agency-sanctioned backup servers?

Further Information

13. Detailed guidance on BYOD considerations and appropriate processes and technical controls can be found in DSD's *Protect* publication *Bring Your Own Device (BYOD) Considerations*. This publication is currently available for Australian Government agencies in draft form through the *OnSecure* web portal.

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

Contact Details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.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.