Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Risk management of enterprise mobility (including Bring Your Own Device)

First published: June 2013
Last updated: October 2021

Introduction

Enterprise mobility enables employees to perform work in specified business-case scenarios using devices such as smartphones, tablets and laptops while leveraging technologies that facilitate remote access to data. A well designed enterprise mobility strategy can create opportunities for organisations to securely improve customer service delivery, business efficiency and productivity. In addition, employees obtain increased flexibility to perform work regardless of their physical location.

This publication has been developed to provide senior business representatives with a list of enterprise mobility considerations. These include business cases, regulatory obligations and legislation, available budget and personnel resources, and risk tolerance. Additionally, risk management controls are provided for cybersecurity practitioners.

This publication aims to assist readers to understand and help mitigate the significant risks associated with using devices for work-related purposes that have the potential to expose sensitive data. Risks are primarily due to the likelihood of devices storing unprotected sensitive data being lost or stolen, use of corporately unapproved applications and cloud services to handle sensitive data, inadequate separation between work-related use and personal use of a device, and the organisation having reduced assurance in the integrity and security posture of devices that are not corporately managed. Additional risks arise due to legal liability, regulatory obligations and legislation requiring compliance, and the implications for the organisation's budget and personnel resources.

Risks can be partially mitigated through a policy outlining the permitted use of devices, including the required behaviour expected from employees, which is complemented by technical risk management controls to enforce the policy and detect violations.

Business cases for enterprise mobility that involve accessing non-sensitive data might permit employees to use their personally owned devices, referred to as Bring Your Own Device (BYOD).

Business cases for enterprise mobility that involve accessing and potentially storing sensitive data might permit employees to use devices that are listed on a corporately approved shortlist of devices. Such devices are partially or completely corporately managed to enforce policy and technical risk management controls. These controls can include preventing unapproved applications from running and accessing sensitive data, applying security patches to applications and operating systems in a timely manner, and limiting the ability of employees to use devices that are 'jailbroken', 'rooted' or otherwise run with administrative privileges. Optionally, some organisations might provide devices to employees, permit a reasonable degree of personal use, and retain ownership of the devices for legal reasons that facilitate the organisation monitoring devices, remotely wiping sensitive data, performing security and legal investigations, and retaining ownership of intellectual property.

Before implementing enterprise mobility for a specific business case, organisations must decide whether applying the chosen risk management controls would result in an acceptable level of residual risk.

Risk management of enterprise mobility

Potential benefits of enterprise mobility

Potential benefits of enterprise mobility include:

- improved customer service delivery, business efficiency and productivity, especially for employees who work out of the office, are field agents or who travel frequently
- improved productivity that is independent of an employee's physical location, and provides employees with the opportunity to be productive when otherwise idle such as when travelling on public transport
- enabling the recruitment of talented people from anywhere in the world who don't want to relocate to the city of the organisation's office
- flexible working hours enabling employees to blend personal time and professional time to achieve an integrated work-life balance
- opportunities to transition employees on extended leave back into the workplace sooner by working part-time from home
- reduced costs of real estate, building operations and building maintenance if employees hot-desk and are encouraged to work out of the office
- business continuity if employees are unable to work in the office, for example due to an air conditioning failure, power outage, public transport strike, flood, fire or other event
- environmental benefits such as reduced commuting to the office and reduced use of printed paper.

Potential benefits of using personally owned devices

Potential benefits of using personally owned devices for enterprise mobility include:

- reduced hardware costs for the organisation if employees pay for their device – an increasing number of employees already own powerful devices and employees might take better care of a device if they contribute their own money towards it
- freedom for employees to use devices that they prefer, are familiar with and have tailored to their usage preferences to increase their productivity
- negating the need for employees to carry a device for work use and another device for personal use
- improved employee job satisfaction, staff retention and recruitment of staff who desire the ability to use their own device
- leveraging modern technologies that empower employees to innovate faster and develop more efficient ways to do their job, by taking advantage of employees who refresh their software and hardware more regularly than organisations that provide outdated IT capability that is refreshed every 3-5 years.

Develop an enterprise mobility strategy

Developing an enterprise mobility strategy is fundamentally important to an organisation successfully implementing enterprise mobility to achieve business outcomes with an acceptable level of risk. In the absence of a strategy, the organisation's mobility might be driven by employees, without clear measures of success and without adequate consideration of risks.

An enterprise mobility strategy might involve starting with a pilot trial consisting of a small number of employees and a business case that is low risk, high value and has clear measures of success. Subsequently reviewing the success of the trial, including the costs and the impact to the organisation's security posture, enables the organisation to make an informed decision as to whether to increase their use of enterprise mobility.

The following sections in this publication provide guidance for the steps associated with implementing the enterprise mobility strategy that the organisation has developed.

Determine the extent of existing enterprise mobility

The extent of existing authorised and unauthorised enterprise mobility can be informed by talking to business representatives and employees, reviewing the organisation's asset inventory of assigned devices, and using controls to detect:

- rogue Wi-Fi access points located on the organisation's premises
- unauthorised devices accessing the corporate network or the internet via the organisation's network
- employees obtaining a copy of organisational data via removable storage media, email or cloud services.

Develop business cases with suitable mobility approaches

Justified business cases for enterprise mobility have tangible and measured benefits to the organisation, its employees and customers. These benefits outweigh the risks and costs to the organisation. Clearly defining each business case, including specifying what organisational data needs to be accessed, provides a better understanding of the opportunities and benefits versus the risks and costs to the organisation.

Example business cases

Organisations developing enterprise mobility business cases might decide to permit employees to:

- collaborate with other employees via instant messaging or video conferencing
- use work-related software including applications developed by the organisation
- send, receive and print work-related emails with file attachments
- access, develop, print, store and share work-related files that reside in data repositories such as SharePoint, network shares or enterprise-grade cloud storage
- access calendars, contacts, intranet websites and intranet web applications
- access the internet using the organisation's network infrastructure.

Example enterprise mobility approaches and scenarios

An example enterprise mobility implementation might involve a combination of the following approaches.

Scenario A

This scenario involves using devices with a hardware model and operating system version that:

- is arbitrarily chosen by the employee
- has minimal risk management controls applied – further details are provided in Appendix A
- is corporately unmanaged
- is used to access the internet via the organisation's network infrastructure.

Scenario B

This scenario involves using devices with a hardware model and operating system version that:

- is arbitrarily chosen by the employee
- has minimal risk management controls applied – further details are provided in Appendix B
- is corporately unmanaged
- is used to access non-sensitive data.

For Commonwealth entities, non-sensitive data is defined for the purpose of this publication as data that is marked as OFFICIAL.

Scenario C

This scenario involves using devices with a hardware model and operating system version that:

- is chosen by the employee from a corporately approved shortlist
- has moderate risk management controls applied – further details are provided in Appendix C
- uses corporately managed separation of organisational data and personal data, for example using remote virtual desktop software, a managed container or partitioning functionality built into the operating system
- uses a corporately managed mechanism to access and potentially store sensitive data, for example using remote virtual desktop software or corporately approved native applications combined with a Virtual Private Network.

For Commonwealth entities, sensitive data is defined for the purpose of this publication as data that is marked as OFFICIAL: Sensitive.

Devices in this scenario might be provided to employees by the organisation, with a reasonable degree of personal use permitted. Organisations might retain ownership of devices for legal reasons that facilitate the organisation monitoring devices, remotely wiping sensitive data, performing security and legal investigations, and retaining ownership of intellectual property. Enabling employees to choose a device from a corporately approved shortlist is

referred to by some vendors as Choose Your Own Device, especially if the device is purchased, owned and managed by the organisation.

Scenario D

This scenario involves using devices with a hardware model and operating system version that:

- is chosen by the employee from a corporately approved shortlist
- has comprehensive risk management controls applied – further details are provided in Appendix D
- is completely corporately managed, for example using Apple Configuration Profiles combined with Supervised Mode
- potentially includes corporately managed separation of organisational data and personal data, for example using remote virtual desktop software, a managed container or partitioning functionality built into the operating system
- uses a corporately managed mechanism to access and potentially store highly sensitive data, for example using remote virtual desktop software or corporately approved native applications combined with a Virtual Private Network.

For Commonwealth entities, highly sensitive data is defined for the purpose of this publication as data marked as PROTECTED.

The comprehensive risk management controls might restrict the device's functionality to an extent that would overly frustrate an employee using a personally owned device. Therefore, devices in this scenario might be provided to employees by the organisation, with a reasonable degree of personal use permitted. Devices on the shortlist might be limited to smartphones and tablets that are part of a single vendor's ecosystem due to the required compatibility with risk management controls. Organisations might retain ownership of devices for legal reasons that facilitate the organisation monitoring devices, remotely wiping sensitive data, performing security and legal investigations, and retaining ownership of intellectual property. Enabling employees to choose a device from a corporately approved shortlist is referred to by some vendors as Choose Your Own Device, especially if the device is purchased, owned and managed by the organisation.

Considerations for choosing enterprise mobility approaches

When selecting an enterprise mobility approach for a particular business case, consider the employee's job role, the sensitivity of the data to be accessed, risk management controls and their impact to employee privacy and user experience. Also consider whether the level of residual risk is acceptable to the organisation, and costs to the organisation such as the level of technical support and financial support provided to employees.

These considerations are represented in Figure 1 which reflects the example enterprise mobility scenarios mentioned previously. Detailed risk management controls for each enterprise mobility scenario are provided in the appendices of this publication.

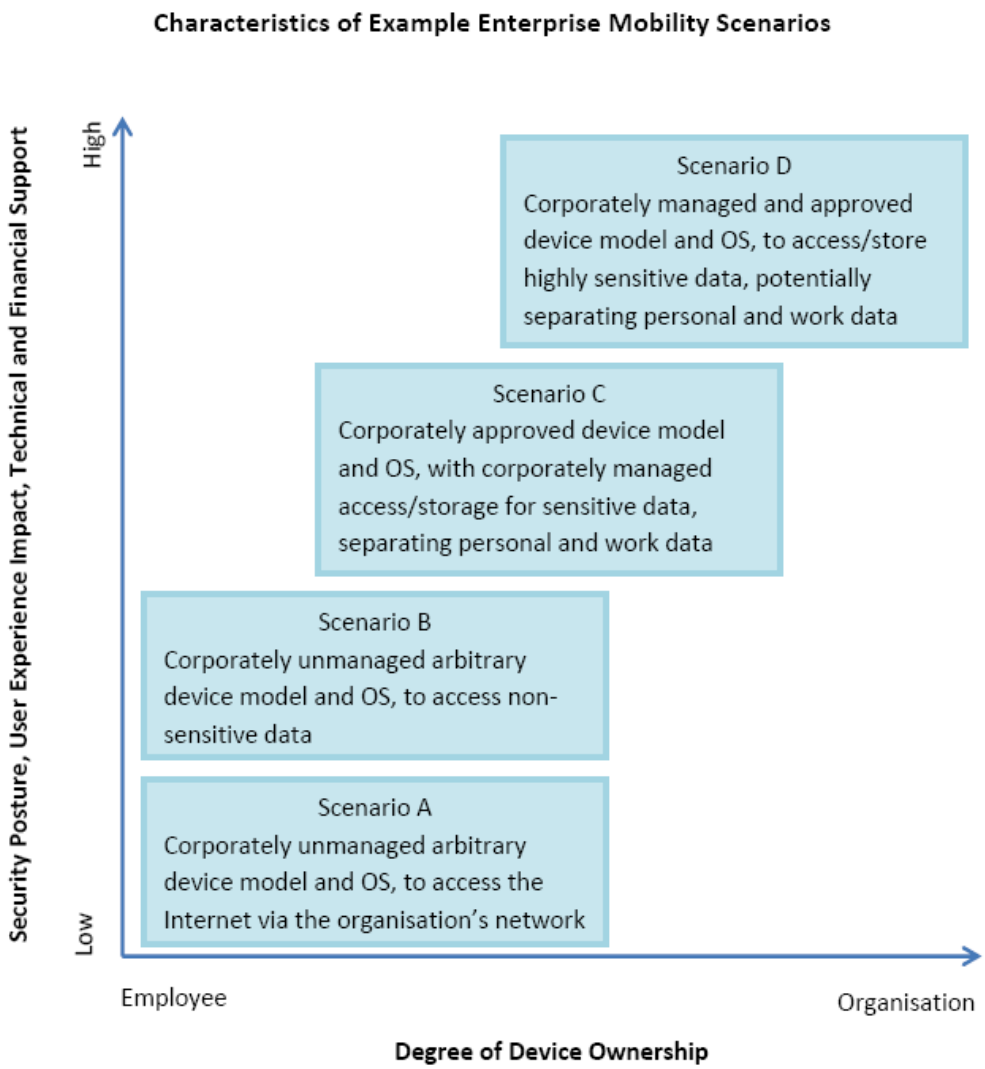

Figure 1. Example enterprise mobility scenarios vary in their suitability to handle sensitive data, their cost and their impact to the employee's user experience.

Identify regulatory obligations and legislation

Legal advice must be obtained before allowing personally owned devices to connect to organisational systems. This publication is not to be considered legal advice.

An organisation's legal representatives must determine to what extent enterprise mobility can be used based on regulatory obligations and legislation affecting their organisation. Relevant legislation includes the *Privacy Act 1988*, state and territory privacy laws including Acts covering surveillance of employees, the *Archives Act 1983* and the *Freedom of Information Act 1982*. Organisations need to maintain an awareness of relevant legislation and address any associated impacts to their organisation.

Aspects of enterprise mobility requiring legal advice might include:

- whether the organisation is permitted to monitor devices and network traffic to identify policy violations and other cybersecurity incidents

- whether the organisation is permitted to monitor the use of personally owned devices outside of the organisation's premises, including remotely locating and tracking a device's location based on the device's GPS coordinates, nearby mobile cell towers or the location of nearby known Wi-Fi networks
- whether the organisation is permitted to access personal data stored on a device when performing a security or legal investigation – personal data includes emails, history of websites accessed, calendar, contacts and photos, as well as personal data stored in the employee's personal consumer-grade webmail or cloud storage account
- what action an organisation should take if violations of civil law or criminal law are accidentally discovered while analysing an employee's device or network traffic
- insurance and liability for compensation, repair or replacement of an employee's device that is lost, stolen, compromised with malware or is otherwise damaged and potentially causes injury – such damage might occur through no fault of the employee's including while using the device in the office for work-related purposes
- legal liability resulting from an organisation remotely wiping personal data, especially if the device is owned by someone who has not provided written consent, such as the estate of a deceased employee
- legal liability resulting from devices spreading malware or otherwise harming other devices
- legal liability to the organisation resulting from employees having or transferring to organisational systems any software or data that is pirated, infringing copyright or is inappropriately licenced
- whether the organisation or the employee owns the intellectual property and copyright of work that is performed on an employee's device, especially if performed outside of traditional business hours.

Allocate budget and personnel resources

Organisations implementing enterprise mobility might encounter a variety of costs such as:

- subsidising or completely paying for the cost of devices and associated work-related expenses
- responding to security breaches, policy violations and regulatory compliance violations
- personnel resources needed from a variety of sections across the organisation to collaboratively develop the enterprise mobility strategy and associated policies
- implementing risk management controls such as licencing security software and user education
- upgrading the organisation's IT infrastructure including the Wi-Fi network, internet bandwidth, as well as the data centre's network, storage and server processing capacity
- personnel to architect the IT infrastructure and perform ongoing device management, monitoring and reporting
- additional software Client Access Licences for Microsoft Windows server and client operating systems as well as for Microsoft Office, especially if the organisation pays for software licences per device instead of per user
- training the IT help desk to support a variety of devices – at a minimum providing employees with configuration settings and basic training to connect to permitted organisational networks and systems
- modifying intranet websites and web applications to support a variety of web browsers

- enhancing identity and access management infrastructure to perform authentication and authorisation of employees and devices
- developing mobile web applications or native software applications to interact with organisational data, potentially requiring the use of middleware solutions enabling access to data storage repositories.

Develop and communicate enterprise mobility policy

Enterprise mobility policy must be developed to govern the use of devices accessing organisational data.

Policy relies on user adherence and is likely to be more effective if it exhibits the following characteristics:

- offers enterprise mobility as opt-in instead of mandatory, unless the organisation is willing to completely pay for the cost of devices and associated work-related costs
- is jointly developed by an advisory board consisting of stakeholders including the cybersecurity team, system and network administrators, human resources, finance, legal, senior management and employees – this consultative process helps to ensure that stakeholders have had input, are willing to adhere to the policy and accept any additional responsibilities to protect organisational data
- clearly states what types of organisational data are permitted to be accessed from which devices and which applications – the absence of an application strategy might result in employees using applications that haven't been assessed by the organisation to determine their potential to expose sensitive data
- clearly states how organisational data is permitted to be stored and distributed, for example using corporately managed data repositories such as SharePoint, network shares or enterprise-grade cloud storage, while avoiding the use of consumer-grade cloud storage and personal consumer-grade webmail
- clearly states which risk management controls apply and deters employees from circumventing these controls by helping employees to understand why policy rules exist
- requires employees to sign an Acceptable Use Policy that clearly states the required behaviour expected from employees and the consequences of violations
- is communicated throughout the organisation to enable employees to understand their obligations and the policy, to ensure full awareness of the existence of the policy and ramifications of non-compliance –the organisation needs to determine which business representatives are responsible for remediating non-compliance, which is complemented by a documented dispute escalation and resolution process
- is complemented by technical risk management controls to enforce the policy and detect violations, especially in cases where an employee dishonours their written agreement to adhere to the policy
- minimises negative impacts to the employee's user experience – negative impacts include requiring a very complex unlock passphrase, automatically locking a device's screen after a very short idle timeout period, excessively limiting a device's functionality, and deleting personal data when wiping an entire device remotely or after a very small number of consecutive incorrect unlock passphrase attempts
- states the technical support and financial support that employees can obtain
- documents the on-boarding process for employees to obtain signed approval from their manager, register their device, have the organisational policy applied, and potentially have software installed on their device to assist the organisation to configure and manage the device

- documents the off-boarding process to remove organisational software and data from devices that are lost, stolen or de-provisioned including when employees cease employment
- provides a business representative point of contact in case employees have feedback about the policy
- is reviewed and refined if necessary, initially on a quarterly basis while enterprise mobility is still new to the organisation, and then on an annual basis.

Surveying employees can help reveal whether they would be willing to accept the policy and participate in enterprise mobility business cases, noting that some employees might perceive that:

- costs will be shifted from the organisation to them
- their privacy will be invaded
- the functionality of their device will be excessively limited
- personal data stored on their device will be deleted or exposed
- they will be expected to be on call to answer emails and phone calls at all times outside of traditional business hours.

Technical support

It is impractical for an organisation's IT help desk to support devices from a large variety of vendors running a large variety of operating systems with a large variety of configuration settings. Therefore, the amount of technical support provided to employees depends on the organisation's personnel resources, whether devices are listed on a corporately approved shortlist of devices, and the degree to which devices are necessary for employees to perform their job. Technical support might include:

- providing guests, contractors and other employees with details of how to connect to the organisation's guest Wi-Fi network to access the internet
- providing employees with details of how to connect to permitted organisational networks and systems, and the organisation obtaining visibility of cybersecurity incidents that place the organisation's data at risk
- providing an internal self-service community support web forum enabling employees to assist each other, with the IT help desk advertising the existence of the internal web forum and occasionally contributing to web forum discussions to answer frequently asked questions – an internal web forum helps to mitigate the risk of employees disclosing details about the organisation's network infrastructure configuration when seeking assistance on publicly visible internet forums
- providing employees with as much technical support as the IT help desk is capable of, including a short term loan of a device to keep an employee productive while they get their damaged device repaired
- providing employees with full technical support, including replacing damaged or broken devices.

Financial support

Financial support might have Fringe Benefit Tax implications due to the organisation paying for a device or internet and telecommunications connectivity that is used for personal use, especially outside of business hours. The amount of financial support provided to employees depends on the organisation's financial resources and the degree to which devices are necessary for employees to perform their job. Financial support might include:

- acknowledging work-related costs incurred in support of employees making tax deductible claims
- providing employees with a taxable allowance or stipend, or otherwise subsidising or reimbursing the cost of a device, contractually obligating employees to repay a pro-rata portion if they cease employment within a set time period
- providing employees with a device that is completely paid for by the organisation, contractually obligating employees to return the device if they cease employment within a set time period or if the organisation retains ownership of the device
- providing employees with reimbursement for the work-related portion of the monthly bill from the employee's telecommunications carrier and Internet Service Provider, noting that rates associated with a consumer plan might be higher than rates associated with a corporate plan
- providing employees with a corporate SIM card or otherwise arranging internet and telecommunications connectivity via a corporate plan, using an automated process to recover the employee's portion of the monthly bill via payroll based on criteria that indicate personal use – expensive data roaming charges for employees travelling overseas can be mitigated by providing employees with a prepaid SIM card associated with a telecommunications carrier in the foreign country, or by disabling data roaming via Mobile Device Management to only allow Wi-Fi data connectivity
- providing employees with reimbursement for the cost of essential work-related software, noting that software licenced to an employee via a consumer licence instead of an enterprise licence is unlikely to be transferable to a different employee
- providing employees with reimbursement for the cost of essential peripherals and accessories.

Monitor the implementation and report to management

Ongoing monitoring of the enterprise mobility implementation includes reviewing logs from Mobile Device Management and other log sources such as network logs, user authentication logs and security software.

Regular reporting to management helps them to understand and address unacceptable risks, and assess whether the benefits of enterprise mobility to the organisation justify the risks and costs to the organisation. Information to report to management includes:

- the degree of compliance with regulatory obligations, legislation and organisational policies
- the severity and number of policy violations and other cybersecurity incidents
- the names of employees who are regularly involved in policy violations and other cybersecurity incidents
- costs of IT infrastructure including network upgrades, internet bandwidth, data storage and server processing capacity
- costs of risk management controls
- costs of providing employees with technical support and financial support
- the names of employees causing an excessive cost burden due to their use of internet bandwidth, data storage, technical support or financial support.

Facilitate organisational transformation

Organisations might update their business processes to leverage enterprise mobility, potentially even transforming the organisation to embrace opportunities such as activity-based working by:

- reviewing the success of enterprise mobility pilot trials, including the costs and the impact to the organisation's security posture
- reviewing and updating the organisation's enterprise mobility strategy
- making an informed decision whether to increase the scope of enterprise mobility to identify and pursue additional innovative cost-effective opportunities to improve customer service delivery, efficiency and productivity with a level of risk that is acceptable to the organisation.

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.

Contact details

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

Appendix A: Arbitrary unmanaged devices for internet access

This appendix provides guidance to manage risks associated with Scenario A. This scenario involves devices with a hardware model and operating system version that:

- is arbitrarily chosen by the employee
- has minimal risk management controls applied
- is corporately unmanaged
- is used to access the internet via the organisation's network infrastructure.

This implementation can enable organisations to apply more stringent web content filtering controls on the corporate network to reduce the risk of corporate workstations becoming compromised.

High level objectives associated with this example scenario include:

- avoid unauthorised access to the organisation's corporate network to help prevent employees introducing malware onto organisational systems or exposing sensitive data
- mitigate the threat of sensitive work-related discussions being recorded by internet telephony, voice recognition or other voice recording applications
- maintain the availability of organisational internet connectivity at an acceptable cost
- reduce the risk of legal liability to the organisation resulting from:
    - compromised devices spreading malware or harming other devices on the internet
    - employees downloading copyright infringing movies, music or software from the internet
    - software or data that is pirated, infringing copyright, or used for work-related purposes even though it is only licenced for home use, non-commercial use or educational use
    - employees accessing pornography or other offensive material while in the office, during working hours, from devices subsidised by the organisation or via the organisation's network infrastructure.

Corporately enforced risk management controls

The organisation is able to manage risk by enforcing the following technical controls.

Filtering and monitoring network traffic

Implement:

- basic internet web content filtering to block access to known piracy, pornographic and offensive websites
- bandwidth throttling and Quality of Service to prioritise work-related network traffic

- bandwidth quotas per user and per device to prevent employees from using excessive bandwidth
- network traffic logging, archiving and monitoring to help identify policy violations and cybersecurity incidents.

Separation between the organisation's corporate network and the guest Wi-Fi network

Separate the organisation's internal corporate network from the guest Wi-Fi network that enables corporately unmanaged and untrustworthy devices to access the internet.

Corporate workstations configured to block access to unauthorised devices

Configure corporate workstations to block access to unauthorised devices, for example USB devices, Bluetooth devices, Wi-Fi access points, mobile hotspots and other devices with 3G/4G connectivity. This helps mitigate the risk of corporate workstations either exchanging data with unauthorised devices, or tethering to devices and accessing the internet via an unmonitored and unfiltered internet gateway.

User-reliant risk management controls

The following technical controls and policy controls to manage risk rely on employees complying with policy.

Anti-malware software

Obtain written employee agreement to use anti-malware software which helps mitigate devices being compromised.

This control is less applicable to devices that use a strong sandbox design and limit the execution of applications to only those that are cryptographically signed by a trusted authority and originate from an application marketplace with a good history of curation to exclude malware.

Additional information

The organisation might offer anti-malware software free of charge when employees access the internet via a captive portal and agree to the policy.

Signature-based antivirus software is a reactive approach that is unlikely to protect against targeted malware that the antivirus vendor doesn't have visibility of. Anti-malware software extends signature-based antivirus software to typically include heuristic detection, identification of applications behaving suspiciously, as well as reputation checking of applications and websites accessed.

Avoid behaviour that is unauthorised, excessive, offensive or unlawful

Obtain written employee agreement to:

- only access organisational systems or data that they are explicitly permitted to access
- avoid sensitive work-related discussions being recorded by internet telephony, voice recognition or other voice recording applications
- use organisational internet connectivity as per existing policy, which might disallow accessing offensive and copyright infringing content, disallow excessive use of internet bandwidth for example via personal use of YouTube, and require employees to accept the risk of their device being compromised

- ensure that their device doesn't contain or transfer to organisational systems any software or data that is pirated, infringing copyright, or used for work-related purposes even though it is only licenced for home use, non-commercial use or educational use

- not deliberately access pornography or other offensive material while in the office, during working hours, from devices subsidised by the organisation, or via the organisation's network infrastructure – Australian Public Service employees are bound by the Australian Public Service Code of Conduct and Values even when working out of the office using their own device.

Appendix B: Arbitrary unmanaged devices for non-sensitive data

This appendix provides guidance to manage risks associated with Scenario B. This scenario involves devices with a hardware model and operating system version that:

- is arbitrarily chosen by the employee
- has minimal risk management controls applied
- is corporately unmanaged
- is used to access non-sensitive data.

For Commonwealth entities, non-sensitive data is defined for the purpose of this publication as data that is marked as OFFICIAL.

This appendix builds upon and incorporates the high level objectives and risk management controls discussed in Appendix A which covers arbitrary corporately unmanaged devices used to access the internet via the organisation's network infrastructure. High level objectives associated with the example scenario in Appendix B also include:

- avoid unauthorised access to organisational systems and data
- avoid untrustworthy devices compromising organisational systems that are permitted to be accessed.

Corporately enforced risk management controls

The organisation is able to manage risk by enforcing the following technical controls.

Segmentation and segregation between devices and organisational systems

Appropriately architect and segment the organisation's corporate network using a combination of security enforcing mechanisms such as firewalls, reverse proxies, Virtual Local Area Networks and Virtual Private Networks. This helps mitigate devices accessing unauthorised organisational systems and data.

Web application and operating system vulnerability assessment and security hardening

Perform vulnerability assessments and security hardening of web applications and operating systems running on organisational systems that are permitted to be accessed. This helps mitigate devices compromising organisational systems and their data.

Appendix C: Corporately approved and partially-managed devices for sensitive data

This appendix provides guidance to manage risks associated with Scenario C. This scenario involves devices with a hardware model and operating system version that:

- is chosen by the employee from a corporately approved shortlist
- has moderate risk management controls applied
- uses corporately managed separation of organisational data and personal data, for example using remote virtual desktop software, a managed container or partitioning functionality built into the operating system
- uses a corporately managed mechanism to access and potentially store sensitive data, for example using remote virtual desktop software or corporately approved native applications combined with a Virtual Private Network.

For Commonwealth entities, sensitive data is defined for the purpose of this publication as data that is marked as OFFICIAL: Sensitive.

Devices in this scenario might be provided to employees by the organisation, with a reasonable degree of personal use permitted. Organisations might retain ownership of devices for legal reasons that facilitate the organisation monitoring devices, remotely wiping sensitive data, performing security and legal investigations, and retaining ownership of intellectual property. Enabling employees to choose a device from a corporately approved shortlist is referred to by some vendors as Choose Your Own Device, especially if the device is purchased, owned and managed by the organisation.

This appendix builds upon and incorporates the high level objectives and risk management controls discussed in Appendix B which covers arbitrary corporately unmanaged devices used to access non-sensitive data. High level objectives associated with the example scenario in Appendix C also include:

- protect the organisation's financial investment in the cost of devices
- maintain the availability and integrity of organisational data for business continuity
- maintain the confidentiality of sensitive data
- maintain corporate ownership of organisational data created by employees using their device
- rapidly respond to policy violations, data spills and other cybersecurity incidents
- be able to perform electronic discovery for litigation cases and freedom of information requests.

Some of the risk management controls described in this appendix might be unnecessary or impractical depending on the organisation's business case, the sensitivity of data accessed by devices, the use of other risk management controls and the type of device noting that some controls focus primarily on smartphones and tablets rather than laptops.

An example shortlist of devices from which employees can choose is a smartphone or tablet device running:

- iOS version 12 or later

- Android version 9 or later running on devices from vendors with a history of distributing security patches in a timely manner.

The shortlist of devices is regularly updated to reflect newly available devices on the market and is limited to only devices that:

- are compatible with required business applications developed by the organisation and by third parties
- the organisation has the technical knowledge to support, resulting in more predictable support costs
- meet minimum requirements specified by the organisation, including compatibility with the organisation's chosen risk management controls such as Mobile Device Management as well as managed separation mechanisms such as managed containers
- provide the organisation with adequate assurance of the device's ability to appropriately protect sensitive data
- comply with Australian legislation and are covered by Australian warranties.

Corporately enforced risk management controls

The organisation is able to manage risk by enforcing the following technical controls.

Overview of managed separation, remote virtual desktop and Mobile Device Management

Devices without Australian Signals Directorate (ASD)-approved encryption should not store sensitive data. Additionally, employees should be prevented from installing unapproved applications that can access sensitive information.

Risk management controls used to follow this guidance include using managed separation such as an encrypted managed container, preferably combined with Mobile Device Management to provide some basic assurance in the device's underlying operating system configuration, or using appropriately configured remote virtual desktop software. Use of the phrase 'remote virtual desktop software' in this publication incorporates virtualised applications and Virtual Desktop Infrastructure (VDI).

Organisations might choose to use managed separation for some business cases such as an evaluated encrypted managed container on smartphones with small screens, and remote virtual desktop software for other business cases or devices with large screens.

Detailed information about managed separation, remote virtual desktop software and Mobile Device Management is provided in the following pages of this appendix. Figure 2 shows the comparative ability of these risk management controls to protect organisational data and their negative impact to the employee's user experience. All of the implementations shown include basic risk management controls such as applying vendor security patches in a timely manner, using up-to-date anti-malware software and performing backups of work data to backup servers specified by the organisation. These risk management controls won't prevent a malicious employee from copying organisational data by taking a screenshot or photograph of their device's screen.

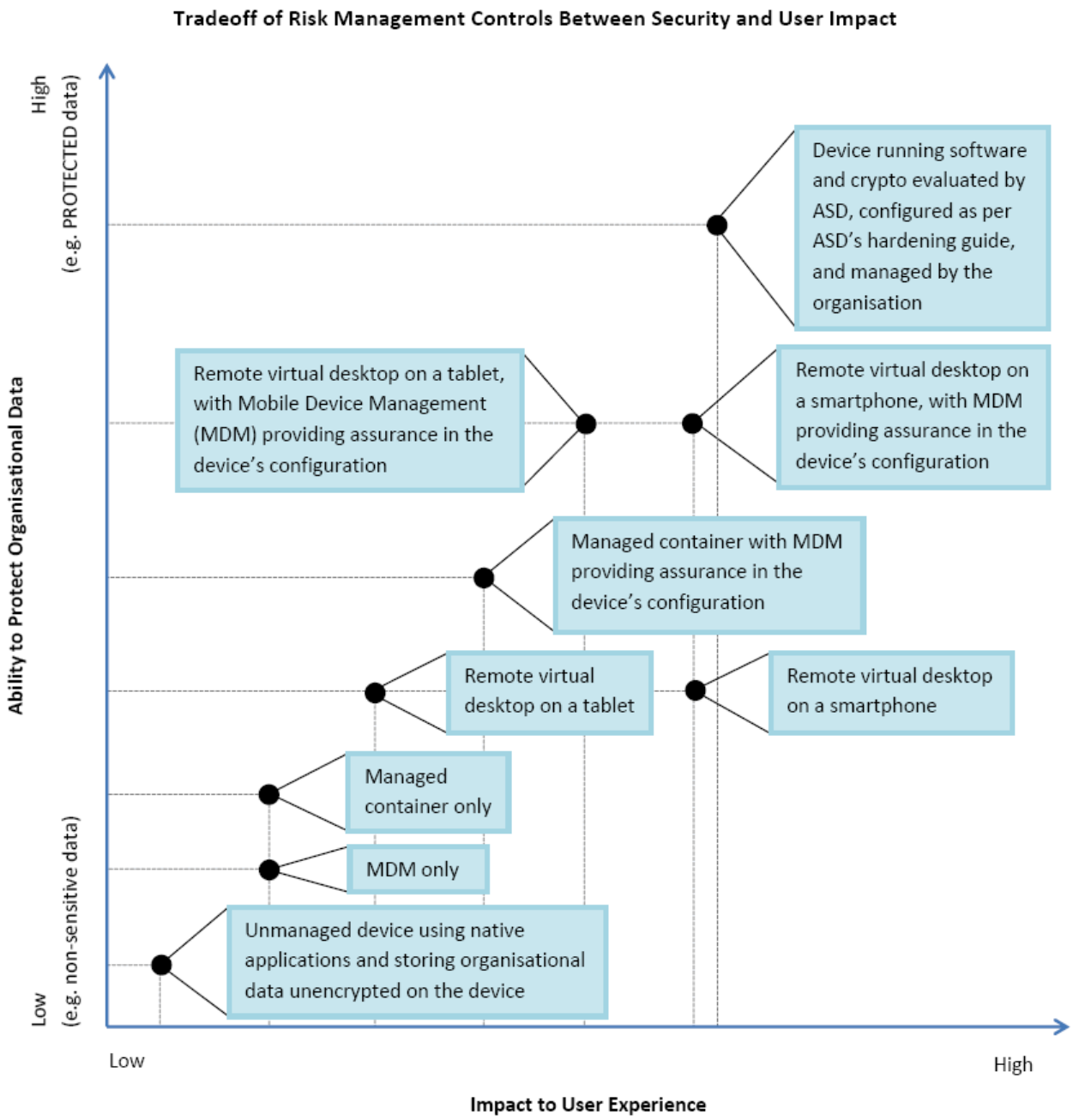

Figure 2. Risk management controls vary in their ability to protect organisational data and their negative impact to the employee's user experience.

Managed separation

Managed separation helps protect and isolate organisational data stored on devices. Organisational data is logically separated from the employee's personal operating environment, limiting the ability of such data to spread, and facilitating the remote wiping of only organisational data.

Additional information

There are several different types of separation mechanisms including partitioning functionality built into the operating system as well as mechanisms bolted on top of the operating system such as managed containers. In addition, technology such as type 1 hypervisors and type 2 hypervisors can provide a locally virtualised operating system. Some separation mechanisms are designed to ensure that organisational data can only be accessed by applications that have been assessed by the organisation.

Managed containers, type 2 hypervisors or other mechanisms bolted onto the operating system provide reduced security if there is inadequate assurance in the integrity and security posture of the operating system.

Use of a managed container has the following corporate benefits with associated potential impacts to the employee's user experience:

- requiring employees to enter an additional passphrase to access organisational data
- data encryption that is independent of the encryption provided by a device's operating system – software-based encryption might slow down the device due to cryptographic overhead
- reducing the risk of data leakage by restricting employees to use only corporately approved applications to handle organisational data, while limiting the ability of such applications to copy organisational data to corporately unapproved cloud services or elsewhere beyond the managed container.

Organisations considering using a managed container need to determine whether the vendor has access to organisational data or cryptographic keys used to decrypt organisational data.

Remote virtual desktop software

Appropriately configured remote virtual desktop software helps keep organisational data in the organisation's data centre and not stored on devices, while still enabling employees to access organisational data and applications.

Additional information

Sensitive data exchanged during the entire remote virtual desktop session must be encrypted using ASD-approved encryption.

Experience shows that remote virtual desktop software does not necessarily keep organisational data in the data centre or prevent such data being transferred to and from devices. Some remote virtual desktop software contains functionality to deliberately enable organisational data to be copied to and from devices, including the ability for malware on devices to be introduced into the remote virtual desktop as shown in Figure 3 below.

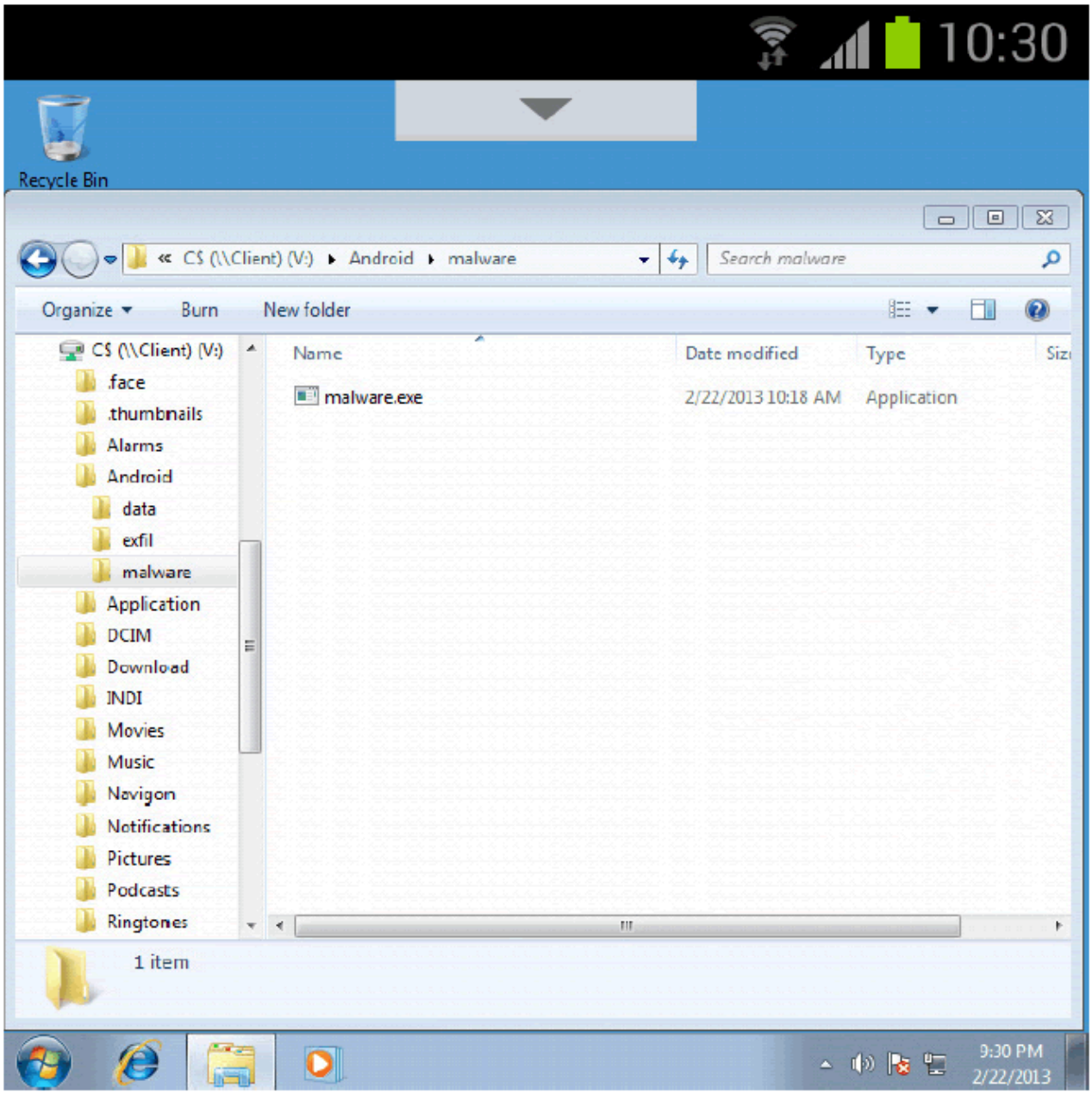

Figure 3. In this example, an employee is accessing their Android device's file system and removable media from within the remote virtual desktop running Microsoft Windows. The employee is able to copy organisational data to their device, and introduce malware into the remote virtual desktop. This employee behaviour results in a less stringent audit trail than if email was used to extract organisational data or to introduce malware.

There are a variety of ways in which organisational data might leak out of the remote virtual desktop and be stored unprotected on devices. Risk management controls to help mitigate such data leakage include:

- appropriately configuring remote virtual desktop software running on the server and on the device to help mitigate the employee printing to local printers, printing to local files, accessing their device's file system and removable media from within the remote virtual desktop, and using the clipboard to copy and paste data in both directions between the remote virtual desktop and the device

- using full device encryption to help protect organisational data that might inadvertently be stored on the device, especially if the device is a laptop due to the possibility of data in memory being written to disk as part of a page/swap file or hibernation/sleep file
- obtaining written agreement from employees to avoid deliberately copying organisational data to their device and to avoid introducing potential malware from their device into the remote virtual desktop
- partially mitigating keystroke logging software and malware that enables malicious actors to take screenshots of the remote virtual desktop by using up-to-date anti-malware software on devices, ensuring that all vendor security patches are applied to devices as soon as they are available from the vendor, and educating employees to avoid installing potentially malicious applications
- configuring the remote virtual desktop to lock its screen after a short idle timeout period to help mitigate malicious actors using a compromised device to control the remote virtual desktop's mouse and keyboard
- disallowing the use of keyboard applications featuring a custom dictionary or predictive text which capture sensitive words or word combinations typed into the remote virtual desktop and save such sensitive data on the device's local file system.

The following impacts of remote virtual desktop software should be considered prior to implementation:

- the requirement for employees to have reliable internet connectivity
- the impact on the employee's user experience especially for devices with small screens such as smartphones, for example, using remote virtual desktop software to turn a smartphone into a dumb terminal might frustrate employees trying to send an email using Microsoft Outlook running on an older version of Microsoft Windows that was not designed for a touch interface
- the potential requirement for the organisation to upgrade their network and data centre's storage and server processing capacity
- the potential requirement for the organisation to purchase additional Client Access Licences for Microsoft Windows server and client operating systems as well as for Microsoft Office.

Mobile Device Management

Mobile Device Management configures and audits devices, including enforcing aspects of the policy such as:

- the device enrolment process, which might involve installing software on the device to assist the organisation to manage the device and a digital certificate to authenticate the device to the network
- unlock passphrases having a specified minimum length and required complexity
- the device idle timeout period until the device's screen is automatically locked
- the number of consecutive failed passphrase attempts until the device is automatically wiped
- the capability to perform remote tracking, locking and wiping of devices
- the ability of employees to print to non-organisational printers
- encryption of data at rest and in transit, including Virtual Private Network configuration settings

- the ability for employees to use their device's camera, microphone, Bluetooth, USB interface, removable media or GPS, particularly while on organisational premises
- detecting, reporting and blocking devices that are jailbroken or rooted, noting that detection is not perfect and relies on an untrusted device to tell the truth about its software
- endpoint compliance checking including whether security patches and anti-malware software are up to date
- disabling the backup of unprotected sensitive data to consumer-grade cloud storage such as iCloud, while still enabling an employee's personal data to be backed up
- configuring appropriate email and Wi-Fi connectivity settings
- disabling inbuilt voice recording applications that send captured voice over the internet
- ongoing device management, monitoring and asset tracking.

Additional information

Mobile devices accessing sensitive data:

- should use Mobile Device Management to ensure that organisational policy is applied, enabling organisations to centrally manage the configuration of devices and audit adherence to policy
- must prevent employees from disabling security functions on a device once provisioned
- should be regularly tested to ensure that devices are still secure, for example that their configuration aligns with the organisation's policy and that security patches have been applied on a regular basis.

Using Mobile Device Management to enforce an organisation's unreasonably strict policy, especially when employee is not using their device for work-related purposes, might negatively affect the employee's user experience.

Organisations considering using Mobile Device Management need to determine whether the vendor has access to sensitive data such as a device's unlock passphrase.

Multi-factor authentication

Multi-factor authentication helps mitigate malicious actors accessing organisational systems by using an employee's compromised corporate user account credentials.

Additional information

Multi-factor authentication must be used for remote access to organisational systems.

Employees should log off organisational systems when finished, so that multi-factor authentication is required to regain access. Organisational systems should be configured to log users off after an idle timeout period.

A physically separate hardware multi-factor authentication token with a time-based value, stored separately to the employee's device, can provide greater security than a soft token such as an SMS or mobile application that displays an authentication token value on the employee's device. If the device is compromised or if its SIM card is reissued to malicious actors, the employee's soft token value can be accessed, thereby defeating the multi-factor authentication mechanism.

Using multi-factor authentication doesn't completely mitigate the risk of malicious actors obtaining an employee's corporate passphrase when the employee types it into a compromised device. Malicious actors could then use this passphrase during a subsequent intrusion, for example by gaining physical access to a corporate workstation and simply logging in as the employee. Alternatively, malicious actors could use a spear phishing email to compromise any employee's workstation on the corporate network and use the previously obtained passphrase to access sensitive data on network drives.

To help mitigate this risk, either require multi-factor authentication for all employee logins including logins to corporate workstations in the office, or require that corporate passphrases entered by employees into untrustworthy devices are different to corporate passphrases entered into corporate workstations in the office.

Encryption of data in transit

Encrypting data in transit helps mitigate organisational data being accessed by malicious actors who have access to device's network communications. Such access might result from the use of a Wi-Fi access point that is unencrypted, or the use of any networking infrastructure that is not controlled by the organisation and is therefore considered untrustworthy.

Additional information

ASD-approved encryption must be used to encrypt sensitive data in transit over untrustworthy network infrastructure. For example, data sent over an untrusted network such as the internet could be protected by using ASD-approved encryption implemented via a Virtual Private Network or remote virtual desktop software. ASD-approved Wi-Fi Protected Access 2 (WPA2) could be used for protecting data that only requires protection when exchanged between a device and an organisation's Wi-Fi access point.

Split tunnelling must be disabled on devices supporting this functionality when accessing an organisational system via a Virtual Private Network.

Remote tracking, locking and wiping

Remote tracking helps to recover a device that has been lost or stolen.

Remote locking and wiping helps to protect organisational data on a device that has been lost, stolen, or de-provisioned including when the employee ceases employment.

Additional information

The consequences of wiping an employee's personal data can be reduced by educating employees to regularly backup their personal data or by using managed separation to avoid wiping personal data in the first place.

Attempting to remotely track, lock or wipe a device that is not network accessible will fail. For example, remote wipe functionality is circumvented if a thief configures a device for aeroplane mode, which can easily be done from the locked screen of some devices.

Successfully remotely wiping a device provides the organisation with a false sense of security if the data has already been accessed or copied by the person who found or stole the device.

Low privileged corporate user accounts

Using corporate user accounts with reduced privileges and limited access to sensitive data helps mitigate malicious actors accessing sensitive data by using compromised employee corporate account credentials or a compromised device.

Additional information

Privileged accounts should not be allowed to remotely access organisational systems containing sensitive data.

Provide a secondary corporate user account, which has reduced privileges and limited access to sensitive data, to employees who either:

- have administrative privileges
- have access to significant amounts of sensitive organisational data
- are at higher risk, for example due to temporarily travelling overseas – such employees might temporarily use a separate corporately provided device.

Network architecture control access to organisational data and systems

Network Access Control helps to implement contextual security to determine if an employee attempting to access organisational data should be permitted based on:

- the device's security posture as determined by endpoint compliance checking, including the degree to which the device is corporately managed
- the employee's identity and the strength of authentication used to prove their identity
- the sensitivity of the data being accessed
- the destination of the data, for example whether data is to be stored on the device or shared via corporately managed enterprise-grade cloud storage
- the employee's network connectivity, for example whether the employee's device is connecting using the organisation's Wi-Fi network or an external less trusted network connection
- the geographic location of the employee and the device
- the time and day of the week.

Devices that don't comply with security policy can be quarantined to have limited internet access but no access to organisational systems.

Devices simultaneously connecting to the organisation's network and an additional network via 3G/4G or Wi-can bridge the two networks thereby creating an additional internet gateway on the organisational network. Risk management controls to help mitigate this include:

- using Mobile Device Management to configure devices on organisational premises to either force all device traffic to an organisational Virtual Private Network endpoint, or to turn off a device's 3G/4G data connectivity while still allowing phone calls
- organisations setting up a custom Access Point Name to control data sent from devices via 3G/4G
- forcing devices to use the organisation's gateway to connect to the organisational network – this also assists the organisation to use existing gateway mechanisms for logging, auditing, and filtering malicious or otherwise undesirable network traffic.

The network flow of sensitive data to devices can be limited by using mechanisms such as Enterprise Rights Management or Data Loss Prevention solutions, for example to prevent a device downloading an email from the organisation's email server if the email or attachment contains specific keywords indicating sensitive data.

Operating system exploit mitigation mechanisms

Limit devices on the shortlist to those devices with operating system exploit mitigation mechanisms such as:

- Address Space Layout Randomisation
- Data Execution Prevention
- applications and security patches that are cryptographically signed by a trusted authority
- application sandboxing to compartmentalise applications, restrict their ability to access data stored on the device, and restrict applications interacting with other applications or the operating system.

User-reliant risk management controls

The following technical controls and policy controls to manage risk rely on employees complying with policy.

Regular backups of work data

Obtain written employee agreement to regularly backup work-related data created or modified by their device, only to backup servers specified by the organisation. This helps mitigate an employee's work being lost due to sudden cessation of employment or their device being damaged, lost or stolen.

Access to email, files and other data of archival significance

Obtain written employee agreement to ensure that work-related data of archival significance is accessible to the organisation. This involves employees using their work email account instead of their consumer-grade webmail account, and using corporately managed file storage instead of storing files locally or in consumer-grade cloud storage. This helps mitigate:

- non-compliance with legislation such as the Archives Act
- corporate knowledge being lost when the employee departs the organisation
- the organisation being unable to properly perform security investigations or electronic discovery for litigation cases or Freedom of Information requests.

Avoid unauthorised cloud services for data backup, storage and sharing

Obtain written employee agreement to avoid exposing sensitive data to consumer-grade cloud services used for webmail, data backup, data storage or data sharing.

Additional information

Some consumer-grade cloud storage and sharing services automatically sync between an employee's devices potentially copying sensitive data to a device that has not been approved to handle such data.

To facilitate the authorised exchange of data between devices, the organisation might need to arrange employee access to a corporately managed and remotely accessible file storage and sharing capability, hosted in-house or by a trusted third party.

Strong passphrase configuration settings

Obtain written employee agreement to use strong passphrases and associated configuration settings.

Obtain written employee agreement to avoid configuring their device's operating system or applications to remember authentication credentials such as corporate passphrases used to access organisational systems.

Additional information

Recommended device configuration settings, based on the sensitivity of data being accessed or stored, are provided by the ISM and security configuration guides such as the *Security configuration guide: Apple iOS 14 devices* and *Security configuration guide: Samsung Galaxy S10, S20 and Note 20 devices* publications.

Cybersecurity incident reporting and investigation

Obtain written employee agreement to immediately report cybersecurity incidents and cooperate with security and legal investigations including providing the organisation with access to their device for forensic analysis.

Additional information

Employees must be directed to report cybersecurity incidents to the organisation as soon as possible.

Cybersecurity incidents requiring reporting include a device suspected of being infected with malware or otherwise compromised, as well as device loss or theft. Additional activities, whilst not necessarily considered to be cybersecurity incidents, that need to be reported by the employee to the organisation include de-provisioning a device for sale or passing to a family member, or if the employee ceases employment.

An organisation's cybersecurity team requires plans and procedures to respond to cybersecurity incidents, for example disabling and monitoring the employee's organisational accounts including Virtual Private Network and remote access accounts, as well as remotely tracking the device and wiping organisational data if appropriate.

Organisations permitting the use of personally owned devices are accepting the residual risks of their use, such as any potential cybersecurity incidents or consequences of legal proceedings including electronic discovery for litigation cases and Freedom of Information requests. Therefore, organisations need to ensure that they have risk management controls to prevent and respond to cybersecurity incidents and legal investigations. Organisations should not assume that ASD has the legal authority and resources to assist with performing forensic analysis or cybersecurity incident response activities that involve personally owned devices.

A security or legal investigation might require an employee to temporarily surrender their device, which the employee might refuse unless required by law, for example due to law enforcement having evidence of a crime to warrant seizing the device. Organisations performing appropriate logging and regular backups of work-related emails and files assists with electronic discovery or other investigations involving employees who refuse to cooperate or who have departed the organisation.

Avoid jailbreaking and rooting

Obtain written employee agreement to avoid jailbreaking or rooting their device to circumvent the protective controls implemented by the device's vendor, which might result in the device being unmanageable by the organisation and easily compromised.

Employee education to avoid physical connectivity with untrusted outlets or devices

Educate employees to avoid allowing connectivity between their device and either a potentially malicious charging outlet or an untrusted device.

Employee education about Bluetooth, Near Field Communication and Quick Response codes

Educate employees to avoid:

- pairing with an unintended or insecure Bluetooth device
- exchanging data with an untrusted Near Field Communication (NFC) device
- scanning NFC tags or Quick Response (QR) codes that are untrustworthy and potentially malicious.

Additional information

Devices storing or accessing sensitive data:

- must be configured to remain undiscoverable to all other Bluetooth devices except during pairing
- must only connect to the intended Bluetooth device during pairing
- must be configured to avoid supporting multiple simultaneous Bluetooth headset connections
- must use Bluetooth version 2.1 or later due to the introduction of secure simple pairing and extended inquiry response which facilitates secure pairing with the desired device – a device's Bluetooth version can be determined by reading the product's specifications or by using the Linux *btscanner* program.

Employee education to avoid installing potentially malicious applications

Educate employees using devices that have an official application marketplace to:

- only install applications from the organisation's enterprise application store or from official application marketplaces such as Apple's App Store, Google's Play Store or Microsoft's Windows Store
- prior to installing or updating an application, determine the risk of exposing sensitive data by reading user ratings, user reviews and the application's requested permissions to ensure that they align with the application's stated functionality – noting that such analysis is not guaranteed to avoid malware.

Educate employees using devices that don't have an official marketplace to obtain software from the official website of mainstream vendors.

Employee education to avoid being victims of shoulder surfing

Educate employees to avoid sensitive data on their device's screen being visible to either:

- people without the appropriate security clearance and need to know
- surveillance video cameras
- members of the public

- anyone, including family members, who are not authorised to see sensitive data.

Additional information

Using a privacy filter on a device's screen might negatively impact the device's touch functionality.

Employee education to avoid common intrusion vectors

Educate employees to avoid:

- sharing their device with unauthorised people who are able to access and expose sensitive data
- sending or receiving unencrypted sensitive data using an untrustworthy Wi-Fi access point, such as a public Wi-Fi access point or any Wi-Fi access point that isn't owned by the organisation
- leaving their device in insecure locations such as an unattended car, checked-in airplane luggage or a hotel safe, especially in a foreign country
- interacting with emails and SMS messages from suspicious or unfamiliar sources, for example clicking on hyperlinks or email attachments
- selecting weak passphrases
- reusing the same passphrase for multiple systems
- unnecessarily exposing their work email address and personal details on publicly accessible websites.

Additional information

All personnel who have access to an organisational system must have sufficient cybersecurity awareness and training including an awareness of social engineering threats.

Security patches

Obtain written employee agreement to apply all vendor security patches for the operating system and applications as soon as they are available from vendors.

Additional information

Mobile devices permitted to access sensitive data should have security patches applied as soon as they become available.

Historically, Apple has provided iOS devices with security patches for at least two years from device availability enabling employees to use devices supported with security patches for the duration of their contract with their telecommunications carrier.

It is comparatively straightforward to apply security patches to some Android devices that don't have third party additions or modifications to baseline Android code. However, applying security patches to other Android devices might be challenging due to the cooperation required from the device's vendor and the employee's telecommunications carrier to tweak, test and distribute security patches. Some vendors and telecommunications carriers might focus their efforts on developing and selling newer devices rather than maintaining the security of the employee's current device, even if the employee is forced to continue using their current device due to a contract

with the telecommunications carrier. Some devices are immediately orphaned and never receive security patches. In addition to vulnerabilities in baseline Android code, some vulnerabilities are introduced by device vendors.

Some cheaper Android devices have the bare minimum hardware specifications required to run the version of the operating system shipped with the device, and might not be suited to running newer major versions of the operating system that require additional memory or processing power. Patching vulnerabilities in the operating system running on such devices might be challenging when security patches are only available in newer major versions of the operating system and are not backported to current and previous operating system versions.

Case study

In 2012, an ASD employee purchased a brand new Android smartphone. The employee subsequently discovered that on the day the smartphone was sold, it contained a vulnerability that at the time had been publicly known for over seven months. The smartphone's vendor and the employee's telecommunications carrier did not make a security patch available.

To demonstrate a targeted intrusion, the smartphone was deliberately compromised by exploiting this vulnerability. The compromise enabled the microphone to be surreptitiously turned on to record nearby audio conversations and the recordings to be transmitted over the internet.

This demonstration highlighted some consequences of organisations permitting the use of devices with publicly known vulnerabilities that the employee is unable to patch. In this case, over 18 months after the vulnerability was publicly disclosed, a security patch still hadn't been made available via the vendor and telecommunications carrier.

Ownership of Intellectual Property and copyright

Obtain written employee agreement that the organisation retains ownership of intellectual property and copyright of work performed on a formally assigned task that the employee is paid to perform, regardless of whether the employee performs the work on their device or outside of traditional business hours.

Encryption of data at rest

Obtain written employee agreement to use full device encryption to help mitigate organisational data being accessed by malicious actors who have physical access to a lost or stolen device.

Additional information

Devices without ASD-approved encryption should not store sensitive data. Also, ASD-approved encryption should be used to encrypt a device's internal storage and any removable media.

Full device encryption doesn't limit which applications can access or spread organisational data stored on the device. Therefore, its effectiveness relies upon the use of additional complementary risk management controls.

Encryption needs to be active when the device is not in use. Depending on the type of device, the effectiveness of encrypting a device's internal storage might be reduced if the device is lost or stolen while it is in sleep mode or powered on and screen locked.

Using software-based encryption might negatively impact the employee's user experience.

Apple's iPads and iPhones use hardware-based cryptographic acceleration for protecting data.

Android version 3 Honeycomb introduced full device encryption, though depending on a device's manufacturer, third party software might be required to encrypt removable media.

Avoid printing via untrusted systems

Obtain written employee agreement to avoid printing sensitive data via untrusted printers outside of the office such as from home, an airline lounge, a hotel or an internet cafe. Otherwise, sensitive data might be exposed to third parties due to printers or print servers storing a cached copy of printouts, or printouts being accidentally left on the printer.

Personal firewall

Obtain written employee agreement to use a personal firewall to help limit the exposure of network accessible services and control which applications can access the network.

Additional information

This risk management control is not applicable to some devices, such as those running iOS, that don't expose personal firewall functionality and avoid using network accessible services. Some devices, such as those running Android, use an inbuilt application permission mechanism to control which applications are able to access the network.

Appendix D: Corporately approved and managed devices for highly sensitive data

This appendix provides guidance to manage risks associated with Scenario D. This scenario involves devices with a hardware model and operating system version that:

- is chosen by the employee from a corporately approved shortlist
- has comprehensive risk management controls applied
- is completely corporately managed, for example using Apple Configuration Profiles combined with Supervised Mode
- potentially includes corporately managed separation of organisational data and personal data, for example using remote virtual desktop software, a managed container or partitioning functionality built into the operating system
- uses a corporately managed mechanism to access and potentially store highly sensitive data, for example using remote virtual desktop software or corporately approved native applications combined with a Virtual Private Network.

For Commonwealth entities, highly sensitive data is defined for the purpose of this publication as data marked as PROTECTED.

The comprehensive risk management controls might restrict the device's functionality to an extent that would overly frustrate an employee using a personally owned device. Therefore, devices in this scenario might be provided to employees by the organisation, with a reasonable degree of personal use permitted. Devices on the shortlist might be limited to smartphones and tablets that are part of a single vendor's ecosystem due to the required compatibility with risk management controls. Organisations might retain ownership of devices for legal reasons that facilitate the organisation monitoring devices, remotely wiping sensitive data, performing security and legal investigations, and retaining ownership of intellectual property. Enabling employees to choose a device from a corporately approved shortlist is referred to by some vendors as Choose Your Own Device, especially if the device is purchased, owned and managed by the organisation.

This appendix builds upon and incorporates the high level objectives and risk management controls discussed in Appendix C which covers devices from a corporately approved shortlist using a corporately managed mechanism to access and potentially store sensitive data. Risk management controls in Appendix C that an organisation considers unnecessary to protect sensitive data are likely to be necessary to protect highly sensitive data. High level objectives associated with the example scenario in Appendix D also include maintaining the confidentiality of highly sensitive data.

Corporately enforced risk management controls

The organisation is able to manage risk by enforcing the following technical controls.

Device selection

Limit devices on the corporately approved shortlist to those devices that are approved by ASD and are configured as per ASD security configuration guides. Prefer devices that have an application marketplace with a good history of curation to exclude malware, for example by analysing applications for suspicious behaviour, requiring applications to

be cryptographically signed by a trusted authority instead of a self-signed certificate, and performing adequate verification of the identity of application developers.

Mobile Application Management and enterprise application stores

Mobile Application Management enables the organisation to inventory, install, update and remove applications and associated data on devices.

Using an enterprise application store enables the organisation to distribute and manage applications developed by the organisation, and assess third party applications to determine their potential to expose highly sensitive data.

Additional information

Employees should be prevented from installing unapproved applications that can access highly sensitive data.

The use of Mobile Application Management and enterprise application stores is a more reliable approach to avoiding the use of applications that might expose highly sensitive data than simply relying on anti-malware software and employees to read user reviews and ratings before installing or updating applications. Allowing only approved applications and updated versions of those applications, or less preferably attempting to identify and block every malicious or undesirable application, helps mitigate devices running applications that either:

- are potentially malicious, undesirable or not approved by the organisation
- have the potential to expose highly sensitive data – this includes adware and potentially unwanted applications that collect data from devices as part of the application's revenue model
- have undesirable interactions with other applications, for example using the 'Open In...' feature to open a highly sensitive email attachment in a consumer-grade cloud storage application.

Some vendor implementations of Mobile Application Management also include functionality to effectively place an application into its own managed container by wrapping it with security policy. Such security policies include:

- requiring a passphrase to be entered before an application will run
- enforcing encryption of an application's stored data
- requiring a Virtual Private Network connection to encrypt an application's data in transit
- limiting an application's ability to copy and paste data.

Mobile Application Management might not be able to block powerful web applications that are written in HTML5 and run within the web browser.

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.

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

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

Australian Government

Australian Signals Directorate