Mobile Cyber Security Guide

Aligned to Cyber Essentials

1 Introduction

CSA Cyber Essentials mark and Cyber Trust mark are tiered cybersecurity standards that are designed to support the cybersecurity needs of a range of organisations.

The Cyber Essentials mark takes on a baseline control approach and is intended to protect organisations against common cyberattacks. The Cyber Trust mark takes on a risk-based approach and is intended to enable organisations to put in place the relevant cybersecurity preparedness measures that commensurate with their cybersecurity risk profile.

Together, the Cyber Essentials mark and Cyber Trust mark provide a cybersecurity risk management framework for organisations.

Globally, mobile devices have continued to proliferate and become increasingly woven into the fabric of our daily lives. Modern mobile devices have transformed how organisations deliver IT services, organisations are shifting to mobile device deployments for organisational business functions[1].

While mobility can enhance performance and productivity, mobile devices bring unique threats to organisations. As organisations embrace mobility, adversaries are refining their techniques to target mobile devices. Mobile threats are growing, and the industry has seen an increasing number of cases targeting mobile devices.

The "Mobile Cyber Security Guide (Aligned to Cyber Essentials)" helps organisations in their defence against mobile-specific risks as mobile device deployments rise and mobile threats become more targeted.

2 Purpose & Intended Audience

The "Mobile Cyber Security Guide (Aligned to Cyber Essentials)" is intended to serve as an implementation guide to accompany the Cyber Essentials mark certification standard, and should be read in conjunction with the Cyber Essentials mark certification standard.

This guide is targeted at organisations keen on securely deploying mobile devices, or organisations keen on strengthening existing mobile deployments.

3 Scope

There are three (3) common types of mobile device deployments: (i) Strict Enterprise Usage, (ii) Corporate-Owned Personally Enabled, and (iii) Bring Your Own Device (BYOD).

Cyber Essentials mark is targeted at smaller or less digitalized organisations that are starting out in their cybersecurity journey, such as Small and Medium Enterprises (SMEs). Correspondingly, this document provides recommendations **scoped to Bring Your Own Device (BYOD) model,** as small organisations tend to adopt such a model.

For other mobile deployment models, organisations may wish to refer to CSA's "Guidelines for CII Owners to Enhance Cyber Security for 5G Use Cases", available at CSA's website.

[1] 2023 Global Mobile Threat Report, Zimperium

4 Bring Your Own Device (BYOD) Mobile Device Deployment Model

Bring Your Own Device (BYOD) refers to the practice of performing work-related activities on personally owned devices. Incorporating BYOD deployments into an organisation can increase opportunities and methods available to access organisational resources, however the increased flexibility and functionality of BYOD mobile devices present unique security and privacy challenges to both organisations and device owners.

To help organisations benefit from BYOD's flexibility while protecting themselves from critical security and privacy challenges, this guide will address the following roles in the BYOD model:

- End user organisation
- Mobile device owner

This approach enables the guide to capture the unique relationship between organisations and mobile device owners in BYOD deployment models. While organisations can implement and enforce various BYOD policies and security controls, mobile device owners remain the "device administrators", with control over installation of applications, device patching/updating, permissions granted to applications, and more. Therefore, the organisation and device owner have distinct roles in managing the security of the organisation and the mobile devices deployed within.

5 Balancing Cybersecurity and Privacy

A crucial factor of a successful BYOD deployment is establishing trust between the organisation and device owner. The integration of personal devices into the organisational environment necessitates a mutual understanding between the two parties, particularly if organisations collect data from employees' personal devices.

Data collection poses a cybersecurity and privacy risk that both the organisation and device owners must address. Managing this risk requires striking a balance, ensuring the security of organisational data while respecting the privacy and autonomy of device owners. Understanding the personal nature of BYOD devices is important when implementing mobile security measures or protocols.

The recommendations in this guide take into account both cybersecurity and privacy risks faced by organisations.

6 References

In preparing this document, reference was made to the following publications:

1. CSA Safe App Standard, Version 1.0
2. CSA Guidelines for CII Owners to Enhance Cyber Security for 5G Use Cases, Version 1.0
3. NIST Special Publication 800-124r2 Guidelines for Managing the Security of Mobile Devices in the Enterprise
4. NIST Special Publication 1800-22 Mobile Device Security: Bring Your Own Device (BYOD)
5. 2023 Global Mobile Threat Report, Zimperium
6. NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0

Acknowledgement is made for the use of information from the above publications.

Annex A: Mobile Cyber Security Guide (Aligned to Cyber Essentials)

Mobile Security Recommendation	End User Organisation Responsibility	Device Owner Responsibility
A.1 Assets: People		
1. User education on mobile-specific threats and best practices **Why is this important:** • With the increase on sophistication and scope of mobile threats, user education is crucial in reducing the likelihood of these threats materialising.	**What should the organisation do:** • Organisations should enable training and awareness efforts by providing the necessary platforms and materials to employees e.g. security exercises, training programs, formal education, etc. • Beyond the inclusion of general cyber awareness training for employees, the organisation should also include topics for business users managing or accessing mobile organisational resources to understand why they play important roles in mobile security, and how they can operate securely.	**What should device owners do:** • Device owners should enhance their education and awareness of mobile threats and best practices. This can include: ○ How to identify phishing attacks ○ How to properly manage authentication credentials ○ Organisation's privacy policy and personal information collected ○ Why apps should only be installed from trusted sources **Additional measures:** • Insight on recent mobile security threats (e.g. phishing scams, malicious applications, etc.) can be found from various sources: ○ Cybersecurity campaigns ○ News forums ○ Global cybersecurity reports
A.2 Assets: Hardware and Software		
2. Mobile Asset Inventory **Why is this important:** • Knowledge of the organisations's mobile environment is the	**What should the organisation do:** • An up-to-date asset inventory of all mobile hardware (mobile devices) and software (mobile applications) assets should be maintained. • Mobile assets within the scope may include the following:	**What should device owners do:** • Device owners should ensure that they have received approval from the organisation before using their mobile device in the organisational environment

Mobile Security Recommendation	End User Organisation Responsibility	Device Owner Responsibility
foundational step to monitoring and protecting the assets within.	○ BYOD mobile devices used in the organisational environment ○ Employees permitted to use BYOD mobile devices ○ Software applications used for organisation's business purposes • Asset inventory lists should contain details of the assets where available: ○ For hardware assets (mobile devices) - hardware name/model, asset type, asset owner, department, approval/authorized date, etc. ○ For software assets (mobile applications) – software name, software publisher, software version, business purpose, approval/authorized date, etc.	
3. Mobile application secure practices **Why is this important:** • With the increase in distribution of malicious applications via various channels, it is important for organisations to ensure their organisation's resources are protected against malware, and for device owners to avoid downloading these malicious applications.	**What should the organisation do:** • Organisations deploying in-house developed mobile applications should distribute apps via a dedicated mobile app store (e.g. Google Play Store, Apple App Store) **Additional measures:** • Applications on mobile devices may be managed using mobile device management systems such as Mobile Device Management solutions, or Enterprise Mobility Management solutions.	**What should device owners do:** • Mobile device owners should only install applications from official application stores (e.g. Google Play Store, Apple App Store) as these platforms have measures in place to detect and remove malicious applications • Mobile device owners should restrict the permissions assigned to each app (e.g. camera access, location access) to only the permissions required

Mobile Security Recommendation	End User Organisation Responsibility	Device Owner Responsibility

	• The following restrictions can be applied to applications on mobile devices depending on how a device is managed and enrolled into a device management system:
	  ○ Restrict which app stores may be used
	  ○ Restrict which apps may be installed via an allowlist or blocklist
	  ○ Restrict permissions assigned to each app
	  ○ Automatically install, update, or remove apps on a mobile device
	  ○ Keep a current inventory of all apps installed on each device
	• Organisations can consider Mobile Application Vetting (MAV) solutions, that typically conduct automated tests and analyses on applications prior to deployment into the organisational environment. This can be applied to both in-house developed and 3rd party applications.	

4. Mobile device security policies **Why is this important:** • Security policies provide a clear course of action for organisations to follow when deploying new technologies, responding to security incidents, remediating issues, etc.	**What should the organisation do:** • Mobile device security policies can be established according to the organisation's security needs. • Mobile device security policies should define device configuration requirements for mobile devices that access organisational data. ○ Organisations may reference suggested secure mobile device configuration guidance from established entities such as Center for Internet Security (CIS)	**What should device owners do:** • Device owners should be made aware of all organisational mobile device security policies prior to deploying or onboarding their mobile device onto the organisational environment, and signal their acknowledgement of the policy.

Mobile Security Recommendation	End User Organisation Responsibility	Device Owner Responsibility

	benchmarks, which are best-practice security configuration guides
	
	• Mobile device security policies should define standards, procedures, and restrictions for end users accessing organisational resources. These policies should address the following domains:
	  ○ Access control – e.g. all mobile devices connecting to organisaitional resources must be pre-approved and in compliance with the organisation's security policies
	  ○ Mobile Device Management – e.g. device owners shall allow the organisation to install software/agents and collect telemetry from the device
	  ○ Security – e.g. device owners must employ reasonable physical security measures to secure mobile devices from being lost or stolen
	  ○ Organisational Protocol – e.g. device owners agree to immediately report to his/her manager on any incident or suspected incidents of unauthorised data access, device loss, data loss, and/or disclosure of company resources, databases, networks, etc.
	• Organisations should regularly review mobile device security policies to prevent weak or outdated security policies.	

Mobile Security Recommendation	End User Organisation Responsibility	Device Owner Responsibility
A.3 Assets: Data		

5. Data Storage & Privacy
 	
Why is this important:
• Protecting the privacy of employees and their personal data stored on their mobile devices is important in enabling the organisation's BYOD policy.
	What should the organisation do:
	• Organisations should clearly communicate BYOD policies to organisational leaders and employees to obtain support and provide transparency in deploying BYOD
	• Organisations should maintain the privacy of employees by:
	  ○ Providing concise and understandable information about what data is collected from mobile devices
	  ○ Only storing or collecting data when necessary for transactions to reduce the impact of potential breaches
	  ○ Securely storing data
	• Organisations should refer to and comply with local data retention laws and regulations when collecting data and telemetry from mobile devices in the organisational environment. Commonly used standards and data retention laws include (but are not limited to):
	  ○ Personal Data Protection Act (PDPA)
	  ○ General Data Protection Regulation (GDPR)
	  ○ Payment Card Industry Data Security Standard (PCI DSS)
		What should device owners do:
		• Device owners are responsible for their own personal data, and should ensure that their personal photos, documents, location information, and other data is kept private and inaccessible to others, including the organisation
		• For storing sensitive data securely:
		  ○ Device owners may leverage device encryption to ensure the confidentiality of their mobile data
		  ○ Otherwise, local storage options such as databases or files on the device itself can be used. This is a less secure option.

Mobile Security Recommendation	End User Organisation Responsibility	Device Owner Responsibility
A.4 Secure/Protect: Virus and malware protection		
6. Antivirus applications for mobile devices **Why is this important:** • Antivirus applications are typically able to conduct malware detection, phishing detection, and network protection, amongst other features.	**What should the organisation do:** • Organisations should encourage device owners to install antivirus applications on their mobile devices. Installation of antivirus applications may also be included as part of organisational mobile device security policies, ensuring compliance before mobile devices are allowed to connect to organisational resources.	**What should device owners do:** • Device owners should install antivirus applications on their mobile device, and conduct regular automated or regular scans to detect and fix any issues • Device owners may take reference to CSA's 5th National Cybersecurity Campaign, which includes a list of mobile antivirus applications that have been tested and assessed on their effectiveness in Singapore's current threat landscape. • Device owners may also install ScamShield, an app that detects scam messages and blocks scam calls
A.5 Secure/Protect: Access Control		
7. Strong mobile authentication **Why is this important:** • Digital identity security threats, such as unauthorized access, impersonation, and other types of fraudulent claims, pose a risk to organisational resources. • It is important for organisations to enforce and employ the appropriate authenticators based on the assurance level required	**What should the organisation do:** • Organisations should implement and enforce strong authentication requirements to access organisational resources. • Organisations should implement Multi-Factor Authentication (MFA) for high-risk transactions using two or more of the following authentication factors: ○ Something-you-Know: Information the user knows such as passwords, PIN, patterns, etc.	**What should device owners do:** • Device owners are responsible for authentication on their personal device, and should enable strong lock-screen authentication such as biometric authentication to prevent unauthorized access to their mobile device. **Additional measures:** • Device owners can consider using credential management tools/software to protect any authentication credentials from unauthorized disclosure

Mobile Security Recommendation	End User Organisation Responsibility	Device Owner Responsibility
to access organisational resources and digital services.	○ Something-you-Have: This requires the user to possess a physical device, application, or token that generates a time-based One-Time Password (OTP) such as software tokens, hardware tokens, etc. ○ Something-you-Are: This involves biometric authentication where the user's unique physical characteristics are used for verification such as fingerprints, facial recognition, etc. ○ Further details on the implementation of the above authentication factors can be found in CSA's "Safe App Standards" • Organisations should implement and enforce policies and practices that govern the use of authenticators, for e.g. implementing a strict password policy that requires users to set strong passwords and rotate them regularly **Additional measures:** • Organisations can consider partitioning the functionality of digital services to allow less sensitive data/functions to be available at lower levels of assurance. • Organisations can consider additional requirements on authentication: ○ Rate limiting to limit consecutive failed authentication attempts	

Mobile Security Recommendation	End User Organisation Responsibility	Device Owner Responsibility
A.6 Secure/Protect: Secure Configuration		
8. Secure mobile connections to organisational resources **Why is this important:** • Secure mobile connections to organisational resources reduce the risk of data breaches, unauthorized access, or eavesdropping of organisational information, all of which could result in financial, reputational, and legal consequences to the organisaition.	**What should the organisation do:** • Organisations should leverage strong encryption technologies such as a Virtual Private Network (VPN) to protect the confidentiality and integrity of the organisation's communications, as well as mutual authentication mechanisms to verify the identities of both endpoints before transmitting data • Organisations should prohibit the use of unsecure Wi-Fi networks **Additional Measures:** • VPNs can assist in ensuring all organisation-approved applications on mobile devices rely on TLS and are unable to be downgraded to HTTP.	**What should device owners do:** • Device owners should not use unsecure Wi-Fi networks when connecting to enterprise resources (e.g. public Wi-Fi)
A.7 Update		
9. Rapid adoption of software updates **Why is this important:** • Software updates provide new features and address newly discovered security vulnerabilities	**What should the organisation do:** • Organisations should enforce the rapid adoption of software updates of organisation in-house developed applications, or any 3rd party applications utilized by the organisation. This can be done via restricting access to organisational resources from devices with outdated applications.	**What should device owners do:** • Mobile device owners should rapidly adopt security updates and patches of applications and device OS

Mobile Security Recommendation	End User Organisation Responsibility	Device Owner Responsibility
A.9 Respond: Incident response		
10. Revocation of access to organisational resources Why is this important: • In the event of a cyber-attack, data breach, or device loss, organisations should have security policies and rules that influence remediation actions for mobile devices • Remediation actions may span a spectrum of possibilities ranging from notifying affected individuals to revoking access to organisational resources	**What should the organisation do:** • Organisations should develop a clear incident response plan that includes remediation actions to be taken in the event of a mobile-related security incident, and ensure that the plan is made accessible to all employees • Organisations should notify users in the event of a cyber-attack or breach via channels such as push notifications or SMS • Organisations should temporarily revoke access to organisational resources of affected individuals and devices while the issue is being remediated to minimise potential unauthorised access to organisational resources by malicious actors	**What should device owners do:** • Mobile device owners who are suspicious that their device may have been compromised should immediately notify appropriate parties such as CISOs, Reporting Officers, or IT support to obtain guidance on the necessary steps to address the issue

Annex B: Additional Cybersecurity Tools

The following table covers additional cybersecurity tools that organisations may consider. These cybersecurity tools will aid in fulfilling the Cyber Essentials clauses.

Additional Cybersecurity Tools	Recommendation

Device Management Systems
• Device management is most commonly implemented via systems such as Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) solutions.
• These systems offer a range of security capabilities, and aid in mitigating threats to the organisation's use of mobile devices, such as information disclosure arising from device loss/theft, insecure access of organisational resources via misconfigured or compromised device, and more
	• Organisations can consider using Device Management Systems such as MDM and EMM, that offer a wide range of capabilities. Organisations should identify the capabilities required to work effectively within their organisation before acquiring a Device Management System.
	• Device Management Systems should minimally be able to:
	  ○ Support the mobile devices deployed in the organisation's environment
	  ○ Enforce security policies on a mobile device, which can configure or restrict the use of mobile functionality and security capabilities
	  ○ Define and enforce user and device authentication
	  ○ Define and enforce protections for data communications and on-device data storage
	  ○ Integrate with the organisation's infrastructure (i.e. any on promise operations, support for a SaaS model, or product certifications/accreditations and 3rd party service integrations)

Mobile threat defence (MTD)
• MTD systems typically are able to detect network-based attacks (e.g. MITM), application-based attacks (e.g. malicious, sideloaded apps), phishing attacks, and more
• These systems can offer multiple remediation approaches in the event of an attack attempt, data breach, or compromised device
	• Organisations should consider implementing Mobile Threat Defence (MTD) systems to detect and protect mobile devices, apps, and end users against attacks.
	• MTD systems should minimally have the following capabilities:
	  ○ Malware detection,
	  ○ Phishing detection, and
	  ○ Network protection (Wi-Fi scanning)
	• MTD systems may be integrated with existing mobile device management systems in the organisation to enable user and administrator alerts, automated response to remediate detected vulnerabilities, or quarantine apps and devices

Mobile Application Development Security • Mobile Application Development Security includes necessary security controls and best practices to better protect applications, and in turn, their end users	• Application development is more commonly outsourced to app developers and providers • If organisations intend to develop their own in-house applications, they should refer to CSA's Safe App Standard which provides a common benchmark and guidance on securing applications and end users against common malware and phishing attempts