Circular No. SRD TR 02/2014

26 Sep 2014

The Chief Executive Officers of All Financial Institutions
The Chief Executives of All Insurers

Dear Sir / Madam

IT SECURITY RISKS POSED BY PERSONAL MOBILE DEVICES

"Bring Your Own Device" (BYOD) is a relatively new practice adopted by a growing number of financial institutions ("FIs") to enable their employees to access corporate email, calendars, applications and data from their personal mobile devices. FIs should be cognisant of the heightened security risks associated with BYOD due to challenges in securing, monitoring and controlling employees' personal devices. FIs should adequately address the attendant risks before implementing BYOD within their organisations.

2 Under the MAS Technology Risk Management Guidelines, FIs are expected to develop a comprehensive data loss prevention strategy to safeguard sensitive or confidential customer information. This includes protecting data processed in end point devices, data in transmission, as well as data stored in servers.

3 It is incumbent upon FIs to conduct a comprehensive risk assessment on the BYOD implementation to ensure that measures adopted sufficiently mitigate the security risks associated with BYOD. Some of the factors which could hinder the effective application of security measures to user owned devices include:

a. Impingement of privacy and personal use
For corporate issued devices, FIs would have the rights to implement data loss prevention measures[1] and restrict the installation of non-authorised applications. In a BYOD environment, employees may rightfully demand the freedom to install applications of their choice on their mobile devices and object to installing certain security software perceived to compromise their personal privacy.

[1] Examples include storage encryption, remote erasure of data, strong user authentication and user activity monitoring.

b. Diverse device portfolio

FIs could standardise corporate-issued devices to a specific brand, model and Operating System ("OS"). In contrast, employers may be obliged to support a wider range of devices, OS and application combinations for BYOD implementation. As such, FIs may face difficulties in ensuring that security solutions are applied across an unwieldy mix of disparate platforms in a consistent and effective manner.

c. Lack of control over device updates

The installation of applications and updates for corporate-issued devices are typically initiated by FIs only after a thorough risk assessment and testing. In a BYOD environment, employees could install applications and perform software updates on their personal devices at will, which may introduce security vulnerabilities or malware into their devices. This may jeopardise the FIs' data and corporate systems which are accessible from these devices.

d. Maturity of Mobile Security Solutions

Many of the security solutions for desktop and laptop have been around for a number of decades, and are well tried and tested. Anti-virus, data loss prevention solutions and intrusion detection software have evolved over the years to become more robust. Although many of the technology and security concepts in the desktop environment can be adapted for mobility, such security solutions are generally still in the nascent stage.

4 Two common ways to address BYOD security are the use of Mobile Device Management and Virtualisation solutions. These solutions can be augmented with other security measures for mobile devices to provide enhanced functionalities:

a. Mobile Device Management ("MDM")

MDM solutions are used to manage and control mobile devices used to access business resources. Before a mobile device is permitted to access the corporate network, the device is verified to ensure that it has not been "jailbroken", "rooted" [2] or compromised. MDM solutions usually come with storage encryption, "lock and wipe" [3] capabilities and can be used in conjunction with other security measures (see examples in Annex 1). MDM solutions could also manage

[2] "Jailbreaking", or "rooting", is the process of modifying the operating system of the mobile device to remove manufacturer-imposed restrictions.

[3] "Lock and wipe" is a security feature that allows a network administrator or device owner to trigger the lock screen or delete data on a computing device under specified conditions. This is typically done through a command sent via the internet to the device. The device could also be set up to automatically delete its data if it does not connect to the Internet or corporate network within a pre-determined period of time, or after a certain number of unsuccessful attempts to unlock the device.

corporate applications, data, policies and settings within a sandbox environment.[4] This aims to allow employees to have unfettered use of the device, while providing enterprises the ability to ring-fence and secure the work environment on the device. A robust MDM solution should be implemented for all BYOD arrangements.

b. Virtualisation
Virtualisation allows employees to have on-demand access to enterprise computing resources and data from their mobile devices using strong authentication and network encryption. Corporate data is not downloaded into the mobile device as it is processed within the corporate datacentre. Strict security policies could also be enabled within the virtual environment to restrict copying and use of peripheral devices, such as printers, removable attached storage, to help further prevent data leakage.

5 FIs should not proceed with the BYOD implementation if they are unable to adequately manage the associated security risks. Should BYOD be implemented, FIs are reminded to remain vigilant and keep pace with technology advancement and emergent threats in the mobility space. Regular vulnerability assessment and penetration testing must be carried out on the BYOD infrastructure to ensure that any security gaps are identified and rectified promptly.

6 Should you have any questions or comments, please contact your respective MAS Review Officers.

Yours faithfully
(Sent via MASNET)
HO HERN SHIN
EXECUTIVE DIRECTOR & HEAD
SPECIALIST RISK DEPARTMENT

[4] A sandbox is implemented by executing an application in a restricted operating system environment to protect the resources (e.g. memory and file system space) that the corporate application may use.

Annex 1

COMMON MOBILE DEVICE SECURITY CONTROLS

S/N	Item	Description
1	User Authentication	When accessing a device on which an authentication policy has been enforced, a user is required to enter a password or PIN. Hardware tokens may also be used as a second factor authentication, if required.
2	Malware defence	Malware defense software refers to antivirus, personal firewalls, Web filtering and anti-spam software.
3	Data encryption	Sensitive data is stored in an unreadable form on devices on which data encryption is enforced. This protects the data against unauthorised access, even if the device is lost or stolen.
4	Whitelisting or blacklisting	Whitelisting is a software control that permits only known safe applications to be executed on the device while blacklisting is used to block specified applications from being executed. Administrators typically blacklist applications known to be malicious.
5	System "hardening"	**"**Hardening" is the process of configuring a computing device such that security risks are reduced. This can be done in a BYOD environment by using the MDM to enforce a lock-screen password on the device and specifying the minimum length and complexity of the password.