COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
Bring Your Own Device Policies and Practices

By Christine Vanderpool[1]

Introduction

According to Statista, in today's world there are almost 15 billion mobile devices in use. According to Microsoft as reported by TechJury, 67% of workers use their personal devices in the workplace, and around 59% of organizations globally have adopted a bring your own device (BYOD) program with as high as 73% in US organizations since just 2018. The impact of the COVID-19 pandemic to the expansion of business adopting a BYOD program is still to be determined, but it is believed by most security professionals that it will increase.

BYOD is defined as the use of personally chosen and purchased devices such as smartphones, tablets, laptops, etc., to execute company or enterprise applications or to access company data. Companies may or may not choose to supply a stipend for such a device or reimburse for data plans used in the process of conducting business on the personal device.

Allowing people to bring their own devices into a corporate environment and network does mean increased risk to the organization. A company should weigh the savings associated with a BYOD program against the risks associated with allowing users to bring their own devices. The risks can be partially mitigated by putting in place the right safeguards. The best safeguard to begin with is a policy that outlines the proper requirements, practices, restrictions, and procedures related to bringing your own device. Other safeguards include tools, processes, and education.

Identified Risks

When an enterprise is building its BYOD guidelines, procedures, and policies, there are several important risks to address. These risks include, but are not limited to:

- Lost or stolen devices
- Data leakage or data loss
- Unauthorized access to data and systems
- Vulnerability exploits
- Malware and other malicious software
- The loss of control of the endpoint, including ensuring up-to-date patches on devices
- Regulation compliance
- Network attacks via unsecured Wi-Fi

Below are additional details for some of the risks to consider; though not all inclusive, they are among the key risks that can exist when moving to a BYOD model.

1. Jailbreaking and Rooted Devices

The first area to address is not allowing the use of jailbroken or rooted devices. Jailbreaking is when a person removes the preset restrictions of the iOS operating system on an Apple device. Rooting is when a person obtains privileged control or administrator-level access for an Android device. Both of these activities can leave the device vulnerable to attacks, which include, but are not limited to:

- Command and control attacks
- Insertion or extraction of files by a malicious user
- Use of key logging, sniffing, or other malicious software to obtain user credentials to critical applications
- Installation of application flaws or malicious or harmful unvetted applications
- Ransomware

2. Subject to Legal Hold

Users can become subject to legal holds. A legal hold is the process an organization follows to preserve all forms (including electronic) of potentially relevant information pertaining to a litigation matter. Preservation of data might require the user to not have the ability to dispose of or change information on the device. It may also require the person to not trade in or wipe the device. If litigation reaches a point of data discovery and data collection, it may not be possible to distinguish between personal and corporate data, which could lead to the collection and discovery of additional data unrelated to the legal matter.

3. Vulnerable Software and Devices

When individuals own and control their own device, they own and control the updates made to the device and the applications on the device, which can mean that known vulnerabilities will not be addressed in a timely manner. Operating systems have regular updates to address issues, which often include security risks. The same is true for applications. It is important to keep both the operating system and all applications on a device up to date with the latest releases. If not, the attacks highlighted above in the Jailbreaking and Rooted Devices section can occur on an unprotected device.

4. Wireless Access Points

Most mobile devices are set up to allow a connection to any Wi-Fi access point or network as soon as one is recognized or found. The device will automatically connect to it without verification of any form. This can be a big risk when the person has company information or data on the device and connects to a network that is not secure. A scenario such as this now presents the opportunity for a man-in-the-middle attack, which could allow someone to use that public access point to get into the company's corporate data and resources.

5. Email Exposure and Cross Pollination

When employees use their personal devices, they will often have multiple email accounts accessed by the device. These accounts are usually loaded into the native email client on the device. The device will have preset configurations to specify what email account to use as the default sender when email is used by other applications, such as photo sharing, texts messages, etc. The person may accidentally send an email to or from a personal email that should have been sent using the company email address or vice versa, which could lead to

data loss or exposures of confidential or sensitive data.

6. Cloud-based Storage Services

Similar to the risks associated with email and data loss prevention are the risks that exist with the use of cloud-based storage services on mobile devices. Data is easily accessible today from anywhere at any time and on any device with the use of cloud-based storage services. It is difficult for an enterprise to control the loss of sensitive or confidential data since the access controls to this information are managed and distributed by the content owners of the data. In addition, most people automatically log in to these applications (they do not enter a user ID and password each time they open an application), which means greater risk of exposure if the device is not controlled by a screen lock or screen password.

7. Lost or Stolen Devices

Losing or having a device stolen can occur regardless of ownership of the device. The big differences between company-issued devices and a BYOD model involve reporting the incident and what additional controls exist to protect what is lost or stolen (e.g., screen locks/screen password controls or device-wiping capabilities). If an enterprise is not made aware of a lost or stolen device, it cannot assess the potential risk associated with the incident and take the proper steps to limit the exposure. In addition, the company may or may not have capabilities to remote wipe the device to remove or, at a minimum, limit the exposure of data loss.

8. Harmful or Malicious Applications

Although the Apple and Google stores do attempt to control what applications are available for download, there are applications that can introduce harmful or malicious code onto the device. Additionally, such applications may request and, with the user's permission given through such steps as acceptance of terms and conditions, gain access to the device's location services, pictures, text messages, etc. The user may be unaware that acceptance allows the device to report back this information to a potentially harmful source.

9. Regulation Compliance

New laws and regulations such as the General Data Protection Regulation (GDPR) are creating new protection requirements around people's personal data. Laws like GDPR focus on the export of personal data outside of certain geographical locations. With BYOD, personal mobile devices can contain access to private personal data for business purposes, and by the nature of being mobile, the device is borderless. Businesses that are subject to such laws that handle personal data must build data protection that complies with the regulations.