Best practices with BYOD

Prepared by:
Paul Dalton, Security Consultant

Table of contents

1. Introduction

In today's modern society the requirement for employees to be based within a corporate office is minimal, largely due to remote working gaining prominence. The cost to provide remote working or mobile technology to employees can, however, be expensive. An ideal solution to this cost issue is enabling the employee to use their own IT and devices. This keeps the cost of equipment down and relieves some of the strain on IT departments by not having to purchase and configure equipment for users. Businesses such as Uber and Amazon Flex have taken advantage of these technological developments as employees only need a motor vehicle and a mobile device to set operate, entirely shifting the technology expenditure to employees directly.

Bring Your Own Device (BYOD) does however bring some risk to an organisation and the security considerations of BYOD are often an afterthought. BYOD bridges work and personal life and, as such, needs to ensure that proper security boundaries between work and personal usage are enforced. Failure to do so could mean that a breach of one environment could lead to breach of the other. Implementing security after an incident, such as a data breach, can be far more costly to an organisation and therefore completely negating the original cost benefit of BYOD. As such, it is important that a baseline best practice, as well as an effective program of security consultancy is executed in order to identify and mitigate risk.

This paper is intended for senior managers and above, with a view to present the overall risks that organisations can encounter with BYOD deployments, as well as touching on some privacy concerns that often arise. Without going into technical detail, this paper will serve to offer suggestions for an overall security baseline that companies should be striving to achieve, relative to the risks that BYOD can introduce, and the technologies or methods that can be utilised to mitigate these risks.

2. What is BYOD?

BYOD is a relatively new concept, starting in around 2012 with slow, cautious adoption. Since then, many organisations have adopted the approach of using BYOD to enable and empower workers to perform their duties more effectively and efficiently, as well as reducing business costs. Studies [1] have shown that employees prefer the use of a single device for both their personal and professional life as it is more convenient and reduces the risk of theft when carrying two devices. Permitting them to use their own device allows them to work more efficiently as they are better acquainted with their personally-owned devices and as they belong to the user they typically take better care of them.

While the benefits of BYOD can seem advantageous, mobile devices do carry threats to the organisation that shouldn't be ignored. Allowing users to bring untrusted devices into an organisation and connect them to corporate resources can have a severe impact on the security of corporate networks. As mobile devices have become more popular, the target for malware has grown larger to the point that the risk is very real and ever-growing. There have been instances of mobile botnets such as the Zeus (Zitmo) botnet that targeted mobile banking and targeted Symbian, Windows Mobile, BlackBerry and even Android [2]. A study conducted by Grand View Research outlined that the growing proliferation of tablets and smartphones will help to fuel the BYOD market, which is predicted to reach $238.39 billion by 2020 [3], rendering BYOD an attractive target for attackers.

While the use of BYOD, as well as Mobile Device Management (MDM) systems (often used to facilitate BYOD deployments) introduces security considerations to the business, legal issues may also arise. Two particularly important laws are the Data Protection Act (DPA) and the Employee Practices Code (EPC). The DPA mandates that employees must take measures against unauthorised or unlawful processing of personal data and the EPC stipulates that employees are entitled to a degree of privacy in the work environment. Many MDM platforms can perform quite invasive auditing upon personal devices, meaning they may contravene the EPC.

3. Security considerations for end-user devices

3.1 Device passcode & security

User authentication and access control security should never be underestimated or under-resourced. This includes, but is not limited to, password policies and authentication, as well as network access controls in order to protect corporate data. The loss of corporate data could range from financial loss to reputational damage and so preventing unauthorised access is of paramount importance. A password policy complying with security industry best practice as well as the needs of the organisation should be enforced upon all devices within a BYOD environment. Allowing users to change their passwords and PINs should also be permitted in order so that users can change their login credentials should they suspect they have been compromised.

The use of containerisation allows an additional layer of security to be applied in the form of a second password (which should be different to the standard device unlock password) to be used to access corporate data. Monitoring of access and authentication should also be considered. This could range from the device locking after three incorrect authentication attempts, to the more serious and drastic scenario of completely wiping the device.

3.2 Application considerations

An often overlooked consideration of BYOD is permitted applications. We often see news stories about malicious apps within the Android Marketplace or the Apple App Store, so this is an important area to consider. When devices are completely corporate owned, software policies can be enforced to allow only a handful of whitelisted applications to execute. When users own their devices this is more complicated. Users typically do not have permission to install software on corporate desktop computers and yet can install as many applications as they would like on their own mobile device. This vast array of applications could bring in unnecessary risk to a business. Effective anti-virus, data loss protection, network threat analysis and monitoring, as well as intrusion prevention and detection can assist in combating the risk of malicious apps. Another often underutilised method of improving assurance in this domain is to engage with users and educate them on staying safe online, while explaining the issues with downloading untrusted software.

3.3 Non-compliance

ideally devices should be compliant with all applied MDM policies and action should be taken against non-compliant devices. Non-compliance can take many forms, such as prohibited applications being installed, out of date operating systems running and no device passcode being active. Devices should be monitored for non-compliance, with a reactive approach towards this. Automated and manual action can be carried out against non-compliant devices, from disabling email access to completely wiping the corporate data from the device.

3.4 Containerisation

Some BYOD solutions offer virtualisation or containerisation of enterprise applications. This application container permits additional security, such as additional passwords to be applied, in order to gain access to corporate information. Additional data loss prevention controls can also be placed on the container to prevent any corporate data from being removed from the extended enterprise perimeter. Along with the additional security benefits, containerisation also allows the segregation of a work life balance as users need to access a suite of apps in order to gain access to corporate data. Another good feature of containerisation is the ability to remotely remove only the enterprise content from the device.

3.5 Tracking

Tracking of devices can be more of an ethical and privacy concern, and less of a security concern. While the ability to track devices could be beneficial in some cases, such as lost or stolen devices (especially company owned devices), users would need to be fully aware that their device can be remotely tracked. The user may not wish for their personal device to be tracked, and so it may be required to add tracking only on certain devices, commensurate with the user's permission for tracking.

3.6 Lost & stolen device policy

At the end of 2016, Kensington [4] published research detailing the following surprising statistics:

- One laptop is stolen every 53 seconds
- 70 million smartphones are lost each year with a recovery rate of 7 per cent
- 4.3 per cent of company-issued smartphones are lost or stolen each year
- 80 per cent of the cost of a lost laptop is from data breach
- 52 per cent of devices are stolen from the home or office, and a staggering 24 per cent from conferences

The cost of a lost device is frequently underestimated as downtime, support and management time is often unaccounted for. Educating users on physical as well as digital security can assist in the prevention of lost or stolen devices. However, ultimately device loss is inevitable. Companies should have procedures in place for dealing with device loss, not only to prevent data breaches but also to assist in getting the user up and running again promptly.

MDM platforms offer the ability to remotely wipe the device, or if containerisation is supported, the removal of enterprise applications. Devices should also be registered with the provider so that the SIM card and device can be barred, ensuring that thieves cannot use the device. Kensington estimate that a well-implemented security policy can assist in reducing the cost of laptop theft by 85 per cent [5].

Users may fear punishment should they lose or have a device stolen, or may not report it as it is not a corporate asset. Users (and the business) need to understand that loss occurs and being prepared for this is vital to ensure the safety of corporate data. It is imperative that a user reports a device lost or stolen in order for the business to act immediately to limit losses and to prevent the spread of any compromise. Any incident encountered should also be used as a learning experience, for both the user and the business, in order to identify any risks or other considerations that may arise.

3.7 Encryption

Many MDM solutions originally offered the ability to encrypt a device's free space, or the entire device. However, there has been a major shift by the mobile operating system vendors. Android devices gained the ability for full-disk encryption from Android 5.0 and file-based encryption became possible from Android 7.0. Apple devices have had encryption built into the hardware and firmware of devices since the iPhone 3GS with notable improvement over the years. This has led to high profile contentious issues, such as the San Bernardino case where Apple refused to assist the FBI in breaking their device encryption [6]. The enforcement of encryption should be considered within a BYOD environment, however, it should be noted that the use of encryption could prevent forensic investigation or file recovery. While this may be ideal in order to safeguard corporate data, this could also prevent a user from recovering personal files and photos from their device.

3.8 Operating systems

Operating systems (OS) are a major security issue for many organisations. A lot of time and effort is invested in their licencing, configuration, deployment and timely patching in order to mitigate software based vulnerabilities and exploits. The latest high profile incident linked to OS security which made headlines was WannaCry, a malware that affected Microsoft Windows desktops and servers. While many issues can be resolved by running the latest software, when the device is owned by the company this is far easier to implement compared to personal devices. For consumer portable devices such as laptops and mobile phones, the choice of OS becomes even more diverse. A key decision in an organisation is the cut-off point for allowing outdated and potentially vulnerable device OS to be permitted within the BYOD environment. One potential solution would be to have a small pool of company owned devices to provide to those users running excessively out of date OS.

3.9 New or dormant devices

An area that is often overlooked is the scenario where a user has an additional device that is unused or has purchased a new device. When users purchase a new device, any business data contained on the old device should be wiped and all access to the corporate environment should be revoked. Additionally, any dormant devices should have their access revoked, or wiped. This ensures that any unused devices do not retain access to the corporate network. Should this device be lost or stolen, as it is only used occasionally, it may be days or even weeks before the user notices and reports it lost or stolen, thus increasing the risk to the business.

4. Security considerations for MDM

The main considerations for MDM deployments are often seen as the benefits and features that the specific platforms provide. All MDM platforms permit the deployment of policies onto end-user devices as well as a centralised portal for management of devices. Beyond this, feature sets become more diverse with some MDM solutions offering accurate GPS mapping of users, the ability to run commands as SYSTEM/ROOT on devices and the ability to deploy onto laptops and tablets in addition to phones.

4.1 Best practice MDM platform management

Most MDM platforms are cloud-based, with few vendors offering virtual machine based options. All serve the same purpose; the over-the-air (OTA) distribution of applications, data and configuration settings for the managed mobile devices. One of the key considerations in any organisation should be the overall security of this platform. Should an attacker be able to gain access to the MDM platform they would have access to all enrolled devices, the ability to track them, deploy apps, read configuration files and more.

4.2 Effective policies

The policies applied to end-user devices need to be carefully planned out. Consideration of the corporate information and services employees need to access is a fundamental part of an effective policy. Policies should apply common sense approaches to end-user devices as well. Enforcing a policy that is far too restrictive on an employee's personal device will only serve to upset them and encourage them to find workarounds to these restrictions, which increases the overall security risk.

While it may seem like a wise approach to devise multiple policies for each department or group of staff, this could also weaken security as it can complicate administration. Having too many policies becomes difficult to manage, implement and audit. It also increases the risk of a policy being applied to the wrong device, which could inadvertently apply a more permissive policy on a user's device that handles highly sensitive or business critical data.

4.3 MDM multi-factor authentication

Most MDM platforms now support multi-factor authentication (MFA). This makes use of not only a username and password, but something that the user has on their person, such as a physical token. This token could be in the form of a smart card, a token, or an authenticator application on a mobile phone. This prevents brute force attacks should an attacker learn a username, or a user has a weak password.

4.4 MDM IP whitelisting

Another good security feature of modern MDM platforms is the ability to restrict access to certain IP addresses or ranges. This prevents anyone without a pre-determined IP addresses from gaining access to the MDM. While this can be an excellent way to protect access to the MDM platform, a consideration would need to be made for home workers, such as out-of-hours helpdesk cover, should a company VPN not be available.

4.5 MDM administrators & users

Much like in domain environments, where the number of administrators and users should be kept to a minimum, MDM platforms should also follow this practice. Accounts should follow the principle of least privilege, giving access only for the required job role. The administrators and users should be regularly audited with accounts being locked for a period of time before being removed, with full auditing and logging enabled.

4.6 MDM enrolment whitelisting

Many MDM solutions now have an added security feature of only allowing permitted devices to be enrolled from certain IP addresses or ranges. This increases the security of the enrolment process as devices must be on the premises in order to join the MDM network. This could pose problems, however, should an employee work remotely and be unable to visit a corporate location for device enrolment.

4.7 Logging & accounting

Logging and accounting doesn't have a direct impact on security but is certainly worthy of mention. Logging and accounting allow clear auditing trails of not only the policies applied to each device, but also any action taken by administrative users of the MDM. This facilitates forensic investigations, as well as internal auditing. It is also possible to audit the applications that are installed on devices, which could highlight key risks or identify malicious applications. However, in a BYOD environment this may be a privacy concern, as users could have applications installed pertaining to heath, religious belief, or sexual orientation for example.

5. Conclusion

Due to the many vendors producing MDM platforms which enable BYOD, there is no single solution or single MDM platform that solves all security issues. Therefore, the choice of MDM platform often comes down to cost or basic function set. As a result, the onus is on the organisation to implement policies in order to protect their networks and user devices. Further to this, these policies must be enforced, tested and audited to ensure they are effective. As the security considerations and risks within an organisation change, so should the policies deployed within the MDM and on user devices. Organisations must also be proactive with their approach.

It is important that users are aware and understand why monitoring and auditing should occur, especially on their personal devices. These security measures should be fully explained and transparent to users as initially they may seem draconian. Also, while users may be under the impression that a lost or stolen device does not cost the business in terms of equipment costs, they should be aware that there is also an attributable cost related to the loss of data, or in the worst case scenario, a breach or attack. Any monitoring and auditing should comply with all necessary laws.

As BYOD gains more traction in the industry, the security challenges will surely shift to reflect this extended, always-accessible corporate network. Consideration of the current security stance, as well as potential future issues, should be carried out and clear policies drawn up. Technical staff need to be mindful of the security threats BYOD can introduce and ensure that policies and procedures are followed, taking action should devices fall out of compliance or be found to be compromised.

Staff may need to be encouraged to use a BYOD programme and effective communication of the BYOD policy can assist in this encouragement. Users should be aware that they have an active part to play in the safeguarding of not only their device, but also the corporate environment which the device will access. Education programmes and security awareness training can assist in enabling users to take a proactive role in reducing risk. This training can also encourage users to take better care of their personal data and devices.

6. References

[1] https://www.tyntec.com/sites/default/files/uploads/tyntec-byod-summary-20150709.pdf

[2] https://www.scmagazineuk.com/zeus-variant-that-targets-the-android-platform-detected/article/559961/

[3] http://www.grandviewresearch.com/press-release/global-bring-your-own-device

[4] http://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches

[5] https://www.kensington.com/en/se/4714/a-suggested-physical-laptop-security-policy-for-private-and-public-organisations-by-kensington-and-idc-policy-download

[6] https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute