advance

MOBILE DEVICES THE THREAT VECTOR OF 2022

WHITE PAPER

INTRODUCTION

Mobile devices have long been a feature of everyday life for most Australians. Whether it's point of sale payments, internet banking, identification, storage of photos and personal information, web browsing, social media, or personal corporate emails, the functionality and simplicity of modern mobile devices have made them a central part of daily life.

Mobile devices are similarly crucial to many businesses—they have enabled remote work in response to the pandemic and allow employees access to corporate data and services while travelling.

Unfortunately, this combination of personal data, corporate data, and access to systems has created a triple bounty for cyber criminals. While IT departments focus on securing perimeters and PCs, many users continue to access systems and data on poorly secured corporate mobile devices, or unmanaged personal smart phones.

This creates an irresistible attack vector for cybercriminals, which often goes unseen by IT professionals, and is set to increase in 2022.

In this paper, we look at the growing threat of mobile devices, how cyber criminals breach them, and how businesses can mitigate this risk.

MOBILE DEVICES
A GROWING THREAT

While they might be a different shape and have smaller components, mobile devices manufactured in 2022 have more processing power than the average laptop in 2017. They are essentially laptops themselves.

Due to ease of use, modern mobile devices naturally end up storing large amounts of valuable data, such as photos, passwords, credit card information, banking details and much more. This alone makes them an attractive target for cyber criminals looking to steal money or extort funds.

With the shift toward working remotely, both business and personal mobile devices have increasingly become a convenient way to access corporate data and services. This could be through locally stored emails, messaging apps such as Teams or Slack, or web browsers accessing SaaS systems like Salesforce. Business-enabled mobile devices can often also access corporate networks holding other valuable assets and data.

Unfortunately, even when corporate oversight is in place, personal devices can be difficult to secure. Mobile device management systems often lack the rich security functionality available for laptop endpoint management.

This treasure trove of personal data, corporate data and corporate access, coupled with lower levels of security, creates a perfect storm for cybercriminals. Usually, they will work through a combination of the following strategies:

1. Once access to a mobile device is achieved, they will start by looking for internet banking or investment apps which they can use to access and steal funds directly.

2. Next, they will look for passwords to personal and corporate services, which can be copied and used later.

3. If this is not possible, they will attempt to steal and delete personal data, such as contacts, photos, etc., and ask for payment to return the data, or in return for not making private information public (e.g., sending personal photos to the user's contacts, or publishing sensitive corporate data in public locations).

4. Cybercriminals may also use the breached mobile device as an access gateway to launch more sophisticated cyber-attacks, such as the propagation of ransomware to a corporate network.

Overall, there is rarely a situation where cybercriminals cannot profit once they have gained access to a modern mobile device. This, coupled with the generally low security of mobile devices and user apathy regarding security measures, creates a growing cyber security threat.

HOW MOBILE DEVICES ARE BREACHED

As previously noted, modern mobile devices are essentially laptops, and that means they can be attacked in many of the same ways.

First off, mobile devices have operating systems just like laptops and desktops. Vulnerabilities in all mobile device operating systems are regularly found, and patches are released to fix them via updates. Unfortunately, operating system updates aren't high on user priority lists, often leaving the door open for cybercriminals to take advantage.

Legitimate apps, once installed on a mobile device, also require regular updates for their bugs and vulnerabilities. These updates are treated with similar apathy by users, and many developers discontinue support for old apps, creating opportunities for cybercriminals.

Malicious apps, just like Malware on laptops, are an attack vector for mobile devices. Cybercriminals create apps which appear to have a legitimate purpose, but in fact steal information, provide remote access, and/or install malware and viruses. While app store vendors try to remove these threats before they reach a wide audience, they face an uphill battle, with more than ten thousand malicious apps removed from the various app stores each day, many of which have been downloaded and installed by multiple victims prior to removal.

Malicious websites can also be accessed through mobile devices causing downloads of malware or redirecting users to install malicious apps.

Finally, social engineering techniques are extremely popular as they are more effective when accessed via mobile devices as opposed to on laptop and desktop computers. This is because many of the signs that would traditionally be red flags are not displayed on smaller devices, and users pay less attention to the finer details and abnormalities. This was most evident in 2021 with the rise of 'missed call' and 'missed package' SMS messages, which contained malicious links designed to trick the user into installing an app which contained a virus designed to steal all information from the device once installed.

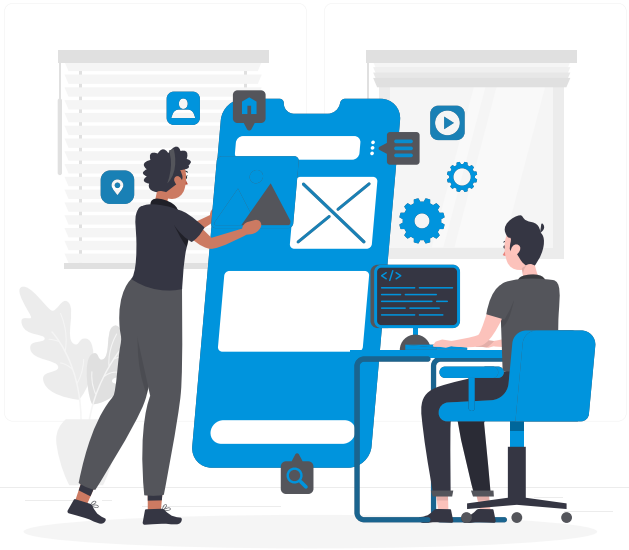
REDUCING CORPORATE RISK
OF MOBILE DEVICES

RE-ASSESS THE NEED

Many modern businesses are re-evaluating the need for mobile devices in their environment. Traditionally, they were the only way for users to access telephony and email services remotely. Technology, however, is changing that. As mobile devices have developed, so have PCs, resulting in most businesses providing users with laptops and enabling remote working. Unless an employee is highly mobile, such as regularly travelling, a laptop usually meets all the requirements of remote access to corporate systems and email.

VoIP technology has also matured, with applications such as Microsoft Teams, Cisco Jabber and Google Hangouts now providing full telephony services to laptops, regardless of location.

Because of this, many businesses are asking themselves, 'If a user can access emails and phone calls with a corporate laptop, what value do mobile devices provide?' Considering the costs of procuring, securing and maintaining corporate mobile devices, or implementing appropriate security across personal employee devices, the balance is increasingly shifting towards retiring mobile device usage in the corporate environment altogether.



CHOOSE THE RIGHT MOBILE DEVICE OWNERSHIP APPROACH

Where a business determines that mobile device usage is worthwhile, it must find a suitable ownership approach. These are often categorised into 'bring your own device (BYOD),' 'choose your own device (CYOD),' 'corporate owned personally enabled (COPE),' or 'corporate owned business only (COBO).'

BYOD allows users to complete business functions on their personal mobile devices. This offers a low upfront investment for the business, and the user benefits from using their device of choice and not needing to carry multiple devices. However, businesses may struggle to implement extensive security controls on devices they do not manage. They may also encounter issues with the shared cost of usage (such as data charges) and the work life balance of the employee.

Modern businesses are finding BYOD is in place even without a corporate decision or oversight, as users take it upon themselves to set up services such as business emails and messaging apps (Teams, Slack etc) on their personal smart phones for ease of use. While often well intentioned, this can present a very significant security risk, as the device has no security standards. Any lost or stolen information is unlikely to be reported, and where it is, the extent or amount is unlikely to be known. This also means corporate data could easily be retained on someone's personal device after their employment has ended.

BYOD is best suited to organisations with limited requirements for mobile devices, such as email and telephony only. Mature policies in usage and data classification are required, as well as strong mobile device management and data loss prevention systems, which can mitigate the risk of unmanaged devices accessing corporate data.

CYOD, the next approach along the spectrum, allows employees to choose from a list of pre-approved mobile devices. For example, a business may offer the choice of several iPhone or Blackberry models, but not Android. Ownership can reside with the business or be transferred to the employee. Either way, it is done so at a reduced cost with the agreement that the business will maintain a level of control over the device for security.

CYOD is best suited to organisations which require mobile devices for a broad range of corporate functions, such as a line of business apps and SaaS websites. These businesses are willing to accept increased cost to provide choices to their employees. CYOD is not a popular approach, as it often ends up producing more negatives than positives for the organisation.

COPE is an approach where the business retains full ownership of the device and its operating costs, with a degree of personal use by the user. It allows for better security control than CYOD or BYOD and avoids any issues with shared operating costs. COPE is usually the default approach of businesses due to a lack of a strong mobile device policy or supporting security controls. COPE has reduced in popularity in recent years, as the personally enabled element adds business risk for very limited benefit. Many employees already have a personal mobile device and are unwilling to retire it when provided a COPE device. In other words, they receive little to no benefit from the personally enabled element of their corporate mobile device.

COPE is best suited to organisations which require mobile devices for a broad range of corporate functions and are willing to offer the latest generation models and generous plans for personal usage. This makes a case for employees to retire their personal devices and can be seen as a perk of employment.

COBO is the most secure and straightforward approach to corporate mobile device ownership. The device is owned and managed by the business, and personal use is not allowed. This allows the business to restrict high-risk functionality, such as non-approved app installations, web traffic filtering, etc. The upfront cost is likely to be greater than BYOD however, the ongoing management effort and cost is likely to be lower.

COBO is best suited to organisations with broad mobile device requirements that want to limit the cost of providing the service. Lower spec affordable devices can be used, and mobile device management tooling can be implemented to reduce ongoing costs without sacrificing security.

While personal ownership approaches, such as BYOD, can often appear commercially attractive due to the reduced upfront cost, personal devices can be expensive to secure, both initially and in the long run.

Even with the right investment in management tooling, personal devices accessing corporate services will always represent a higher level of risk. Users cannot be prevented from installing apps, and they are ultimately responsible for updating and maintaining certain elements of the device, such as the operating system. From a long-term perspective, these strategies often cost significantly more to operate than corporate ownership.

COBO often benefits from the best security posture and lowest operating cost. Unfortunately, it also requires the greatest upfront cost, and results in users physically carrying two separate devices.

Businesses need to select the right ownership approach based on an assessment of activities for which mobile devices will be used, the data and access they require, and the level of security necessary for each device.

ACCEPTABLE USE POLICY

The next item in the corporate toolbox for protecting against mobile device threats is the acceptable use policy. This policy documents usage guidelines once an approach to mobile device ownership and use has been determined.

While this doesn't provide any technical security controls, it represents an agreement between the user and the organisation regarding activities they are, and are not, allowed to carry out on their device. This is used to formally document any requirements, limits, and/or restrictions (such as personal use, updating of apps and OS, and installation of unapproved or non-business apps) and reduces the likelihood of users undertaking high-risk activities. The acceptable use policy's primary goal is to make users aware of their obligations and restrictions in using the device, and repercussions for misuse.

MOBILE DEVICE MANAGEMENT AND TECHNICAL CONTROLS

Mobile device management (MDM), sometimes referred to by its umbrella terms, 'enterprise mobility management (EMM)' or 'unified mobility management (UMM),' is the tooling put in place to enforce the guidelines of the chosen ownership approach and acceptable use policy.

Consolidating desktop/laptop management tooling with mobile device management tooling can be an effective way to streamline activities. Wherever possible, controls implemented for mobile devices accessing corporate systems should be similar to those implemented for laptops.

The security threat presented by modern mobile devices is usually mitigated through the following controls:

- Enforced and monitored operating system updates
- Enforced and monitored application updates
- Enforced and monitored mobile device anti-virus products
- Web traffic filtering
- Enforced password protection, minimum password standards, and encryption
- App blocking and whitelisting
- Public Wi-Fi restrictions
- Device tracking and remote wipe functionality
- Corporate or personal data containerisation

Implementing effective mobile device management on personal devices can be extremely difficult and depends on the user proving permission. On corporate owned devices, the requirements for security controls extend beyond protection of the organisation, as they also have a corporate responsibility to protect their employees and provide safe working equipment.

USER TRAINING

Possibly the most effective technique for securing corporate and personal mobile devices is education and awareness. Almost all bad security practises by users are developed through a lack of awareness rather than intentional negligence. By providing ongoing training on good practices and habits, businesses can greatly increase their security while also protecting employees during their personal use of mobile devices.

CONCLUSION

In both personal and corporate spheres, access provided to, and data stored on, modern mobile devices are increasing every day. Unfortunately, practices of users and security features of management systems for mobile devices continue to lag behind those of desktop and laptop computers. This creates malicious opportunities for cybercriminals to profit, and they are taking notice. In 2022, more than ten thousand 'missed call' and 'package delivery' SMSs were sent to Australians every hour, in one of the most visible examples of cybercriminal behaviour in the mobile world.

As usage trends of mobile devices continue to grow, so will the cybercrime trends. Seeing how this trend is playing out in the corporate sphere as well, with both sanctioned and unsanctioned mobile device usage, businesses must step up their game. It is their responsibility to determine if and how mobile devices will be used in their organisations, communicate this to their users, and implement policies and technical controls to manage this usage actively.

Contact Info

+61 8 8238 6500

sales@advance.net.au

www.advance.net.au