Mobile Security

Dr. Bhawana Rudra
NITK

- Disclamer: The information provided in this presentation are considered from various sources of the web.

Mobile is everywhere:

5 Trends with significant implications for the enterprise

1

Mobile is primary

91% of mobile users keep their device within arm's reach 100% of the time

Source: "China Mobile 50k survey"; Morgan Stanley Research; 2011

2

Insights from mobile data provide new opportunities

75% of mobile shoppers take action after receiving a location based messages

Source: JiWire Mobile Audience Insights Report Q42011

3

Mobile is about transacting

96% year to year increase in mobile cyber Monday sales between 2012 and 2011

Source: IBM Coremetrics Retail Data – as published in 11/24/12 IBM Press Release

4

Mobile must create a continuous brand experience

90% of users use multiple screens as channels come together to create integrated experiences

Source: Time, Inc. 2012

5

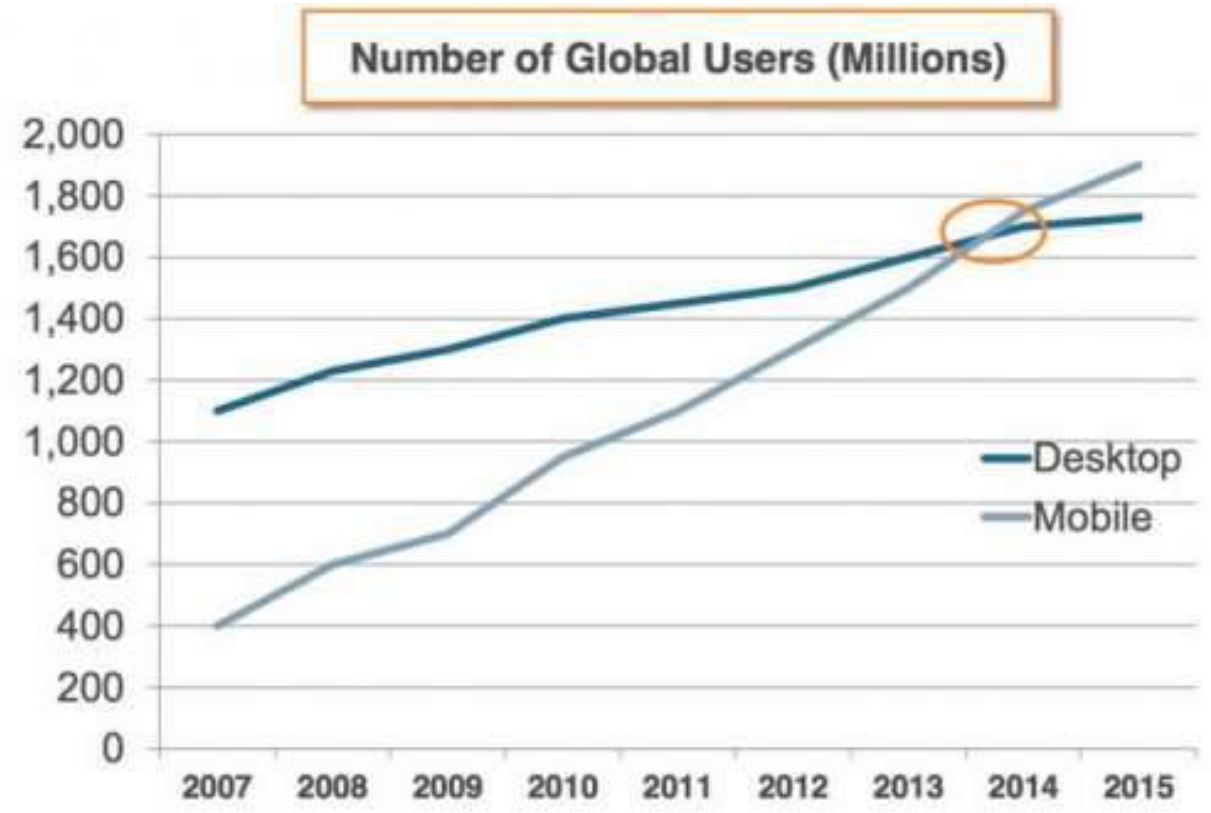
Mobile enables the Internet of Things

Global Machine-to-machine connections will increase from 2 billion in 2011 to **18 billion** at the end of 2022

Source: GSMA, Machina Research

Introduction

- Mobile phones are considered as secured until lately:
- Nov 2009 Ikee, the first **worm targeting jailbroken** iPhone was discovered.
  - Not really malicious: all it did was replace the wall paper of the phone to a picture of the singer and internet meme Rick Astley
- A few weeks later, a truly malicious worm appeared which was designed to steal the user's online banking credentials
  - Targeting only jailbroken iPhones
- March 2010 3000 Vodafone's HTC Magic devices found to have the **Mariposa Botnet malware** installed via the phone's memory card
- June 2010 **Brute-force attack** on 100.000 iPad users who had their email addresses stolen via a vulnerability in a feature on AT&T Website.


Number of Global Users (Millions)
2,000
1,800
1,600
1,400
1,200
1,000
800
600
400
200
0
2007
2008
2009
2010
2011
2012
2013
2014
2015
Desktop
Mobile

- July 2010 Netquin, a mobile security company, claims 100 000 Symbian devices impacted by a Botnet virus that sent messages containing URLs linked to mailicious sites to all the contacts of the address book
- July 2010 LookOut Mobile Security's Apps Genome research finds that 14 percent and 8 percent of free apps available on iPhone and Android can access people's contact data.
- August 2010 on iPhone malicious code can be hidden in fonts that automatically load when the user opens a PDF file, allowing hackers to take control of the device
- Aug 2010 Kaspersky identified the first **Trojan horse** targeting Android devices that sends SMS to premium-rate numbers
- Multiple Android malware were discovered but relatively confined
  - Downloaded from 3rd party appstores and not Google's.

- Spring 2011 DroidDream appeared:
- The **DroidDream Trojan gained root access to Google** Android mobile devices in order to access unique identification information for the phone.
- Once compromised, a DroidDream-infected phone could also download additional malicious programs without the user's knowledge as well as open the phone up to control by hackers.
- DroidDream affected mobile devices running v2.2 (FroYo) and earlier versions of the Android OS operating system
- Entered phones through the download and installation of one of 50+ third-party applications that were available on Google's official Android Market.

- Google removed the apps from its marketplace
- • Had to utilize its "kill switch" to remotely wipe Android devices that had been infected by DroidDream.
- DroidDream got its name from the fact that
  - it was set up to run between the hours of 11pm and 8am
  - when users were most likely to be sleeping and their phones less likely to be in use.
- Additional variants of DroidDream have since appeared
- DroidDream Light in June 2011
- A variant of DroidDream Light that appeared a month later

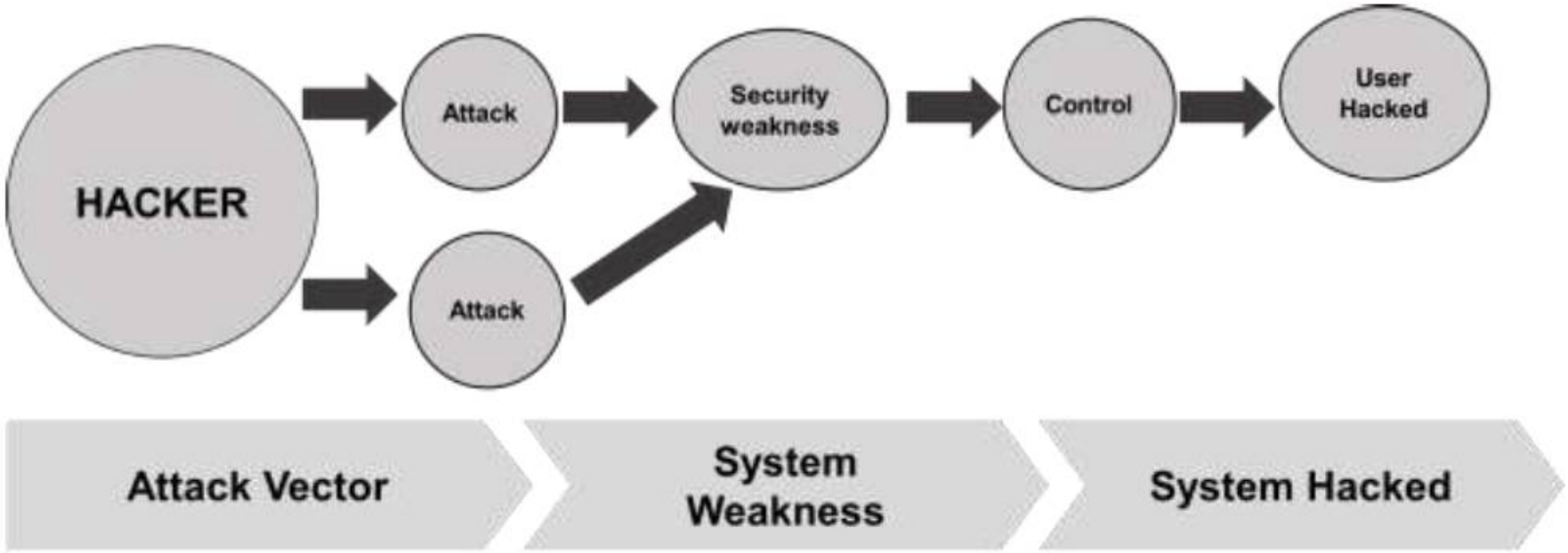
	Passwords	Smart Cards	Biometrics	Pattern Lock
Security	Weak	Strong	Strong	Weak
Ease of Use	Easy	Medium	Hard	Easy
Implementation	Easy	Hard	Hard	Easy
Works for phones	Yes	No	Possible	Yes

Why

- In recent years, mobile devices have been used increasingly in organisations to improve productivity with the Ministry of Defence looking to leverage this trend to enhance its operational efficiency.
- The estimated number of mobile devices is around 5.8 billion, which is thought to have grown exponentially within five years and is supposed to reach nearly 12 billion within four years. As per 2016, per by now it has increased so high.
- Many users **aren't even aware of the security risks with** mobile devices--making them fairly easy targets in many cases.
- The security tools **is not as mature or** sophisticated as it is for PCs
- However, the use of mobile devices also opens up new areas of vulnerability for potential adversaries to target.
- Mobile threats can largely be divided into several categories such as physical, network-based, system-based and application-based threats.

Mobile Security – Attack Vectors

- **Attack Vector** is a method or technique that a hacker uses **to gain access** to another computing device or network in order to inject a "bad code" often called **payload.**



Conti...

- Some of the mobile attack vectors are:
- Malware
  - Virus and Rootkit
  - Application modification
  - OS modification
- Data Exfiltration
  - Data leaves the organization
  - Print screen
  - Copy to USB and backup loss
- Data Tampering
  - Modification by another application
  - Undetected tamper attempts
  - Jail-broken devices
- Data Loss
  - Device loss
  - Unauthorized device access
  - Application vulnerabilities

Thinking Through Mobile Management and Security

IBM Mobile Management and Security Strategy

- Management and safe use of smartphones and tablets in the enterprise
- Secure access to corporate data and supporting privacy
- Visibility and security of enterprise mobile platform

At the Device

Enroll
Register owner and services

Configure
Set appropriate security policies

Monitor and Manage
Ensure device compliance and mange Telecom expenses

Reconfigure
Add new policies over-the-air

De-provision
Remove services and wipe

On the Network

Authenticate
Properly identify mobile users

Encrypt
Secure network connectivity

Monitor and Manage
Log network access and events manage network performance

Control
Allow or deny access to apps

Block
Identify and stop mobile threats

For the Mobile App

Develop
Utilize secure coding practices

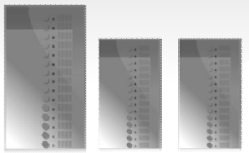
Test
Identify application vulnerabilities

Monitor and Manage
Correlate unauthorized activity and Manage app performance

Protect
Defend against application attacks

Update
Patch old or vulnerable apps

Corporate Intranet



Physical Threats

- It is important to protect devices unattended. In addition, device authentication and encryption need to be enforced to protect mobile devices against unauthorised access.
- It allows an attacker to perform malicious actions such as flashing it with a malicious system image that is connected to a computer to install malicious software or conduct data extraction.
- LOST OR STOLEN DEVICES
- The most basic threat to physical device security is also the most common, loss or theft. Biometrics and kill-switches are reducing the incidence of mobile device theft, but still tens of millions of smartphones are lost or stolen every year.
- Once a laptop, tablet or smartphone is in the hands of a determined criminal, given enough time, a data breach is almost assured.
- From 2005 to 2015, more than 41% of all data breaches were the result of lost or stolen mobile devices (laptops, smartphones and USB drives).

Mitigation

PREVENTION / MITIGATION

Strong Password Policies	Enforce complex device passwords to prevent unauthorized parties from using manual/brute-force techniques to guess the password and gain access to the device.
Enforce Encryption	Encrypt data to prevent extraction from the device. For example, a device's external SD card may be removed and read via an SD card reader. However, if the SD card is encrypted that data is essentially unusable.
Disable USB (applicable for Android and Windows devices)	Disable USB to prevent access to sensitive information via USB debugging, prevent side loading of malicious files/programs and prevent download of information from the device's storage.
Real-time Location Services (RTLS)	Configure geographic boundaries for company-owned devices. If the device leaves the approved area, an EMM solution can automatically lock it down, wipe sensitive/confidential information and/or notify appropriate personnel. Also, manually lock lost/stolen company-owned devices and enable location tracking to retrieve the devices.
Kiosk/Lockdown	Lockdown the user interface of the device to prevent access to apps and settings that may compromise the functionality of the device, or the data on the device and to improve the user experience.

Network-based Threats

- Mobile devices use common wireless network interfaces such as Wi-Fi and Bluetooth for connectivity. Each of these interfaces has its own inherent vulnerabilities and is susceptible to wireless eavedropping attempts using readily available tools like Wifite or Aircrack-ng Suite.
- Users should thus only connect to trusted networks using WPA21 or better network security protocols.
- Attackers attack by compromising the standard operating system through Rooting (Android) and Jailbreaking (iOS). Recent research found that 0.1 % of enterprise iOS devices are Jailbroken and 0.5% of enterprise Android devices are Rooted. This may not sound threatening, but when you consider the pool of hundreds of millions of devices, the danger is real.
- Smartphone operating systems can be intentionally compromised by the user, or it can occur as a side effect of malware. Either way, the Jailbroken or Rooted device is less secure and more vulnerable to attack. Key issues include:

Mitigation of Jailbreak/Root Detection

- Updating and patching the OS becomes more difficult, if not impossible. This can leave many nasty security exploits on the device.
- A Rooted or Jailbroken OS will compromise the device's app isolation capabilities, aka sandbox.
- This can potentially allow malicious apps to affect other apps and access their data.

Apps can be downloaded from third-party app stores, but there is no guarantee that the downloaded apps are clean and free from malware.

PREVENTION / MITIGATION

Jailbreak/Root Detection	An EMM agent will block enrollment and notifies the IT manager if a device is Jailbroken/Rooted.
Wipe Content	An EMM solution's secure document manager and secure browser will block access to content and wipe downloaded content if the device is jailbroken/rooted.
OS Patching/Updating	Identify and segregate devices running old/vulnerable OSs and limit the settings and apps pushed to the devices until they receive suitable OS updates. An EMM solutions will force an OS upgrade or deploy the appropriate OS patches.
Integration with Device Attestation Services	An EMM solution integrates with device attestation services to verify the integrity of the hardware, firmware and OS. Create compliance/alert rules to revoke access to work content, settings and apps upon detection of device attestation violations.

MAN IN THE MIDDLE ATTACK

A main function of any mobile device is communications, but not all mobile communications are secure and private. A man-in-the-middle (MITM) attack can listen in, or even alter the traffic going to and from a mobile device. The most common way for this to happen is over public, unsecured WiFi networks.

There are hundreds of millions of WiFi networks around the world of which almost 1/3 are either unsecured or poorly secured. It is easy for a cyber criminal to setup a fake WiFi hotspot (honeypot), then intercept and manipulate the stream of data. Even the most secure WiFi network is attackable. In late 2017, there was a lot of buzz about KRACK (Key Reinstallation Attack) which exploited a serious weakness in the WPA2 protocol used to secure WiFi networks. KRACK could be used to steal usernames, passwords and other sensitive corporate content.

Other network types are equally at risk. Cyber criminals (and law enforcement) can use fake cellphone towers (aka stingrays) to spoof 2G/3G/4G connections. In addition, most modern mobile devices running Android, iOS, Linux and Windows can be attacked through Bluetooth. In both situations, the device data stream is compromised and malware can be introduced.

PREVENTION / MITIGATION

Whitelist WiFi Access Points	Pre-configure devices with approved WiFi access points and restrict the device user from creating new WiFi connections or modifying existing WiFi connections, effectively creating a white list/safe list of WiFi access points to which the device can connect. Each WiFi configuration in the white list will be configured to ensure compliance with corporate encryptions and security standards.
Disable Bluetooth Pairing	Mitigate Bluetooth vulnerabilities by temporarily disabling Bluetooth communications
Disable Access to Websites with Invalid SSL/TLS Certificates	Prevent MITM attacks by using an EMM secure browser to avoid connecting to sites with certificates that are untrusted, expired or do not match the site name.
Configure and Enforce VPN/ per-app VPN	Configure and enforce VPN and/or per-app VPN connectivity to secure communication even over insecure/ compromised networks.

- **Network Spoofing Attacks**
  - **Rogue WiFi hotspots and Bluetooth devices can be used to** intercept and tamper with the network communication to the smartphone.
  - Rogue Internet gateway names may be configured on the smartphone by a malicious SMS configuration message. In this attack, a spoofed service configuration **SMS is used to change the default access point used by the phone**
  - A more complicated spoofing attack relies **on mounting a rogue GSM base station. The hardware required to set up such** a base station has become relatively inexpensive. This attack is not feasible on 3G networks because of network integrity keys.

- **Network Spoofing Attacks**
  - A rogue WiFi hotspot or other spoofed network nodes can be used as a means to carry out several other attacks, e.g. phishing, SSL downgrade attacks, eavesdropping, etc (making it less likely using 3G networks)
  - Theoretically speaking, such attacks should be detectable by the user.
  - However, in practice most users **do not pay attention to trust cues such as SSL certificates or whether a site uses SSL4.**
  - For smartphone users the risk is even higher because **security indicators (such as a 'trusted SSL connection' indicator) are harder to find or missing on smartphones.**

- **Network congestion**
- As a network device smartphones can be used to provoke network congestion in two ways:
  - **Signalling overload: always-on smartphone apps are** constantly polling the network for updated information.
  - For every bit of data sent, a large number of signalling messages are sent (e.g. keep-alive messages). A typical smartphone generates 8 times more signalling traffic than a laptop with a USB dongle
- **Data capacity overload: Cisco estimates that mobile data** traffic will double every year through 2014, increasing 39 times between 2009 and 2014 (33).
  - Mobile data traffic will grow at a compound annual growth rate of 108 percent between 2009 and 2014, reaching 3.6 million terabytes per month by 2014
  - An attack mobilizing a large number of mobile phone can make the mobile network collapse.

- **Distributed malware attack**
- Although not yet targeted
- Smartphones could be used to launch distributed attacks, just as traditional PCs are now used as parts of larger botnets.
- Smartphone botnets could be used for familiar crimes such as **spam, click fraud and DDoS.**
- Since smartphones interface with cellular networks, they could also be used for new distributed attack scenarios e.g.
  - **SMS spam and DDoS on telephony networks.**
  - Mobile phone coverage is becoming increasingly vital, especially in the event of an emergency, so smartphones open up new possibilities for DDoS attacks with potentially serious impacts.

System-based Threats

- Manufacturers can sometimes introduce vulnerabilities into their devices unintentionally.
- For instance, the SwiftKey keyboard in Samsung Android devices was found to be vulnerable to eavesdropping attempts.
- Security updates were subsequently released to fix the issue (SwiftKey, 2015).
- Similarly, there exist critical vulnerabilities in Apple devices' iPhone Operating System (iOS).
- One example is the "No iOS Zone" vulnerability that automatically connects any iOS devices within range to a fabricated network and repeatedly crashes the device to deny its use (Amit, 2015).
- This vulnerability was eventually fixed in a later version of the iOS.
- These incidences highlight the need to perform timely updates of mobile devices to mitigate system issues.

Application-based Threats

- Using outdated software increases the risk that an attacker may exploit vulnerabilities associated with these software.
- Attackers usually use social engineering techniques to trick users into installing these malicious applications.
- It can be in the form of a link in a message, a shortened hyperlink or a repackaged application that masquerades as a legitimate application.
- It is therefore essential that controls be enforced on the download and installation of applications.

MALWARE

Historically, malware has been a greater threat to desktop and laptop PCs than mobile devices. However, because mobile devices are becoming more powerful and ubiquitous, mobile malware is growing at six times the rate of desktop malware.

Malware is the catch-all term for dozens different types of potentially harmful applications (PHA). The most common are:

Trojans; A type of malware that hides as something else such as a legitimate piece of software. Once a Trojan has been installed, many things are can happen; opening a backdoor, rooting/ jailbreaking, keylogging/spying, and spreading botnets for DDoS attacks.

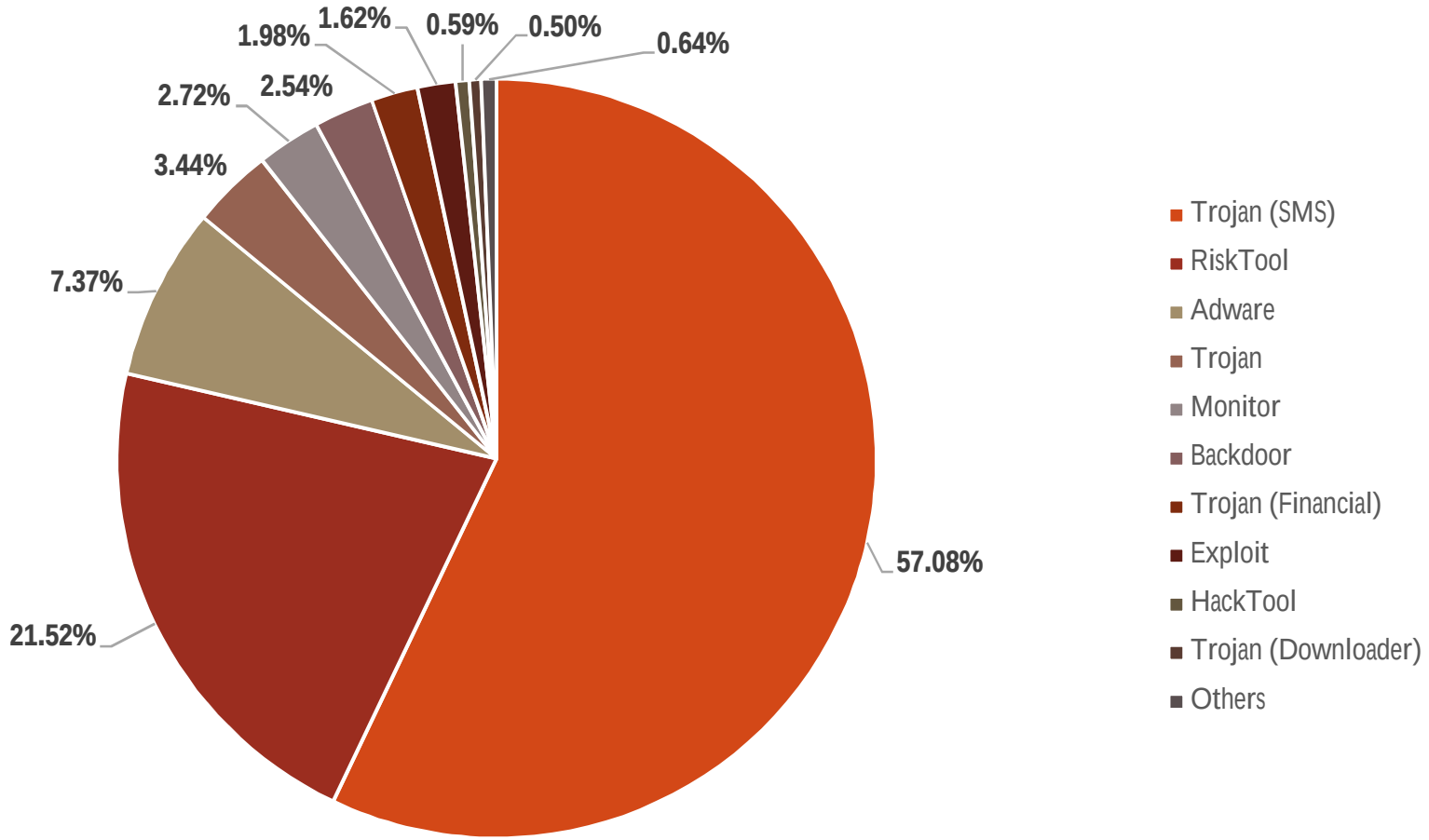
Ransomware; It can be the effect of a Trojan, phishing or hacking, but the result is the same. An external user takes over and locks down something you need, whether it's important data or a critical system. You are then required to pay money, usually in the form of untraceable Bitcoins, to unlock your data and resume normal operations. Mobile ransomware is one of the fastest growing categories of malware, increasing by a factor of 3.5 between late 2016 and early 2017.

Adware / Clickware; There is a "less evil" category of malware that acts to generate revenue by secretly clicking on banners from paid ads. In 2017, a malware codenamed "Judy" was found in several Korean games. It is estimated to have been downloaded more than 10 million times and at its peak was generating over $300k per month in ad revenue.

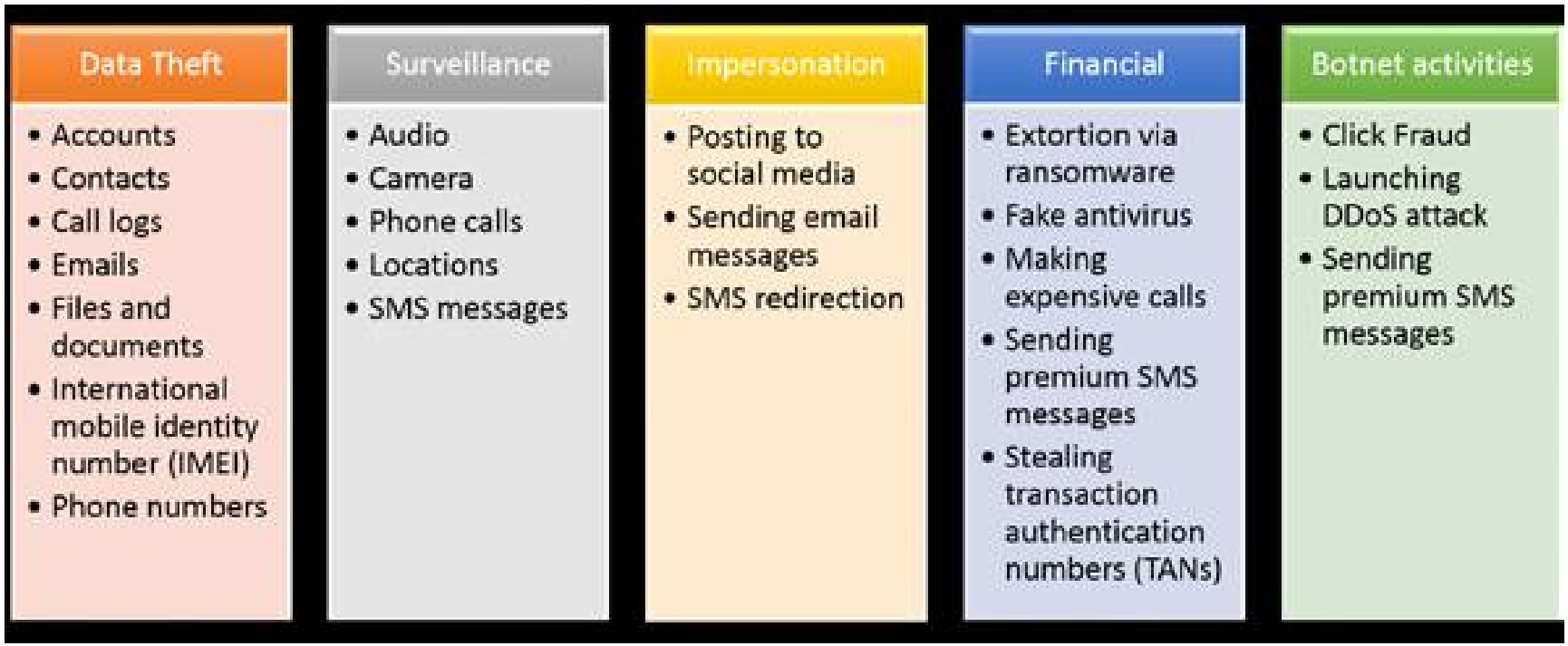
PREVENTION / MITIGATION

Antivirus Protection	Use an antivirus solution that is either built-into, or integrated with, an EMM solution to secure your devices. An integrated antivirus solution can offer scanning, quarantining and deleting of infected files or apps, as well as detection and remediation of malware at the time of file download or app installation.
Whitelist/Blacklist apps	Define a list of apps that can/ cannot be installed and run on devices, limiting your company's exposure to PHAs.
Prevent Installation of Untrusted Apps	Create approved enterprise app catalogs that device users can use to install pre-approved public app store and in-house apps. Prevent end-user side loading of apps (via USB) or installation of app from unauthorized app stores.

Malware Types



- What a Malware Can Do?



- **Spyware attacks**
  - Malicious software that
    - Covertly collects information about users and their activities
    - To use it for marketing purposes, such as profiling or targeted advertisements.
    - Often apparently bona fide software,
    - Installed with the user's consent
    - Which requests and abuses privileges over and above those required for the stated purpose of the app.

PHISHING / SOCIAL ENGINEERING

An up and coming concern for corporate security is the growing threat of social engineering and phishing attacks. Phishing attacks are easier to create and require less skill than coding Trojans. They rely on human nature rather than on sophisticated code. This explains why globally the number of phishing attacks has increased by 65% in a single year.

Smart criminals are leveraging personal information they have acquired illegally to improve the effectiveness of phishing attacks against individual targets (spear phishing). It is easy to see why a majority of surveyed business professionals consider phishing / spear phishing and social engineering as their top security concern. No matter how careful the IT department is, a misguided employee can easily circumvent any preventative measures and make the corporate network vulnerable to criminal activity.

PREVENTION / MITIGATION

Web Filtering	Use an EMM secure browser and whitelisted / blacklisted domains or categories of sites to minimize the chances of a user accessing a malicious or compromised site.
Disable Access to Websites with Invalid SSL/TLS Certificates	An EMM secure browser will block access to sites with invalid certificates – this is common with malicious websites posing as familiar trusted sites.

DATA LEAKAGE

Not every threat to corporate security is from an external cyber-criminal. Another significant source of security breaches is from insiders, be it accidental breaches, intentional breaches or those arising from stolen credentials. In the US, the first half of 2017 saw a 13% increase in the number data breaches, but there was a staggering 164% increase in the number of records lost, stolen or compromised. The scary part is that although only 18% of reported data breaches are due to unintentional loss, they accounted for 86% of the total records lost.

Data leaks are especially damaging in regulated industries such as retail, healthcare and finance. For regulated industries, data breaches can result in significant fines, litigation or at the very least, a damage the company's brand and reputation. In the EU, data loss prevention (DLP) will become even more important after the GDPR rolls out in May 2018 across the EU.

PREVENTION / MITIGATION

Multi-factor Authentication	Use multiple modes of authentication (passcode, biometrics, ID services) to confirm the end user's identity before enrolling the device and deploying settings and software.
Certificate-based Authentication	Mutual certificate-based authentication establishes trust between managed devices and the EMM server. Provision devices with identity certificates to secure access to company resources, such as WiFi and VPN.
Secure Email Gateway	Use an EMM email gateway to secure on-premise MS Exchange email and ensure email can only be accessed from managed and compliant devices.
Content Management Apps	Use an EMM solution's secure document manager and secure web browser to prevent sharing of sensitive information within corporate files and websites. Encrypt corporate files and web content on the device, and wipe downloaded content when a device is retired, rooted or jailbroken.
Enforce Separation of Work and Personal Data and Apps	Prevent sharing of data from company apps and emails accounts to personal apps and emails accounts on the device.

BYOD

The growing trend of bring-your-own devices (BYOD) is both a boon and a bane to business. On the plus side, BYOD can save a company money and keep workers happier and more productive. It lets employees keep in touch with their friends and family throughout the workday via messaging and social media. With all of these benefits, it is no wonder that industry experts are projecting that the global BYOD market will reach $366 billion (USD) by 2020, up from $30 billion (USD) in 2014.

The negative side of BYOD is security. For IT managers, mobile devices are already considered the weakest link for corporate security, unmanaged or uncontrolled devices just make it worse. They show an increased likelihood to suffer all the threats previously identified. More malware, more phishing and more data leakage. The only security threat that decreases is lost or stolen devices. People tend to take care of their own devices better than work devices. Especially when they are on the hook for a replacement.

PREVENTION / MITIGATION

Formal BYOD Policy	Around 60% of companies have formal BYOD policies. Even in the absence of EMM, a BYOD policy can reduce many security risks.
Secure Email Gateway	Use an EMM email gateway to secure on-premise MS Exchange email and ensure email can only be accessed from managed and compliant devices.
Content Management Apps	Use an EMM solution's secure document manager and web browser to prevent sharing of sensitive information within corporate files and websites, encrypt corporate files and web content on the device, and wipe downloaded content when a device is retired, rooted or jailbroken.
Enforce Separation of Work and Personal Data	Prevent sharing of data from company apps and emails accounts to personal apps and emails accounts on the device.

IOT SECURITY

If scale and complexity are significant contributors to mobile security risk, then the Internet of Things (IoT) multiplies that risk a thousand-fold. As the IoT ramps up, so does the need to secure and manage the endpoints. Experts forecast that over 23 billion connected 'Things' will be in use by 2018, tripling to more than 75 billion by 2025. That's 75 billion endpoints delivering essential functionality at the edge of your network – sensors, actuators, printers, scanners, wearables and robots, as well as a many more 'things' that we don't even know about yet.

Historically, IoT devices have had poor security and are attractive targets for cyber criminals. In late 2016, hackers compromised thousands of poorly secured IoT endpoints to create a botnet that executed a massive DDoS attack on a key part of the internet infrastructure. This was only the first of many large cyber attacks that used IoT devices as the attack vector.

PREVENTION / MITIGATION

Full Lifecycle Management	Because they are at the edge of your network and often unattended, IoT endpoints need to be secured just as much as enterprise mobile devices, if not more so. Having visibility into these endpoints in your EMM solution will give you the ability to secure and manage them throughout their full lifecycle, from deployment to retirement.
Strong Password Policies	Weak or unchanged default passwords are often exploited by malicious parties. Enforce complex password policies to prevent unauthorized parties from using manual/brute-force techniques to guess the password and gaining access to the device.
Patching/Updating OS and Apps	An EMM solution can identify and segregate devices running old/vulnerable OSes/apps and even force an OS/app update. On IoT devices, this capability is critical as they often lack the device manufacturer, carrier or app store services that are used to update mobile OSes and apps.

A CORPORATE MOBILITY POLICY

Popular clichés about IT security include; "security is a journey, not a destination," or "there is no silver bullet." On the surface, they may seem trite, but there is a lot of truth to these statements. No single initiative will guarantee mobile security, and you will always be trying to hit a moving target. An effective enterprise mobile security strategy involves multiple approaches and continuous improvement.

The best place to start is with a corporate mobility policy. It will answer important questions such as, who within the company should get what type of mobile device? What apps do workers need? Who gets access to what documents and files and from where?

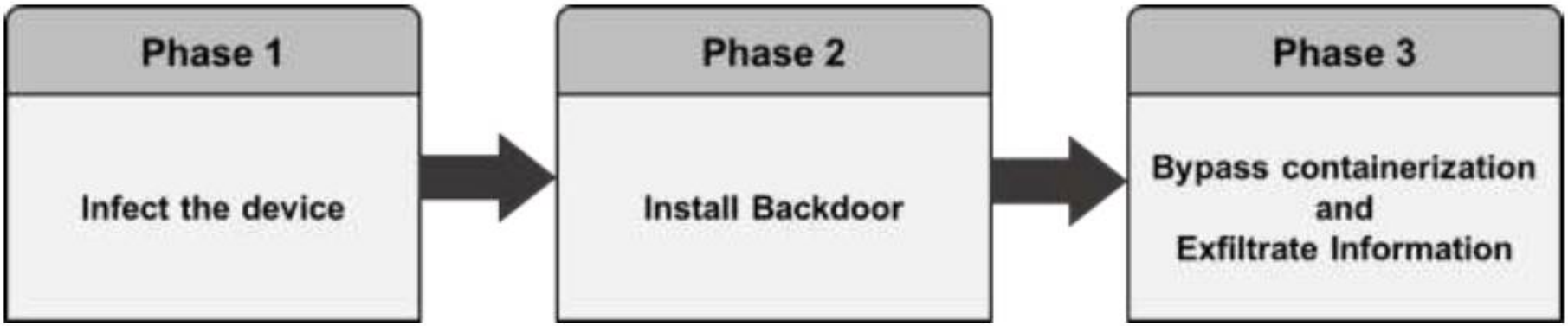
BYOD is such a big and important topic that many companies have a separate BYOD policy. Alternatively, do you only allow corporate-liable devices (COPE, COBE, CYOD), or shared devices for shift workers? How you deploy your mobile devices and what they get used for is a critical element of your corporate mobility policy.

Once you have created your policies and educated your workers, the best way to enforce it is with an enterprise mobility management solution. EMM brings your corporate mobility policy to life. It controls device security, manages who gets what apps and content, and fixes device problems remotely. Together, a corporate mobility policy and an EMM solution deliver a one-two punch that KOs most cyber criminals.

Consequences

- Attack vectors is the hacking process as explained and it is successful, following is the impact on your mobile devices.
- **Losing your data:** If your mobile device has been hacked, or a virus introduced, then all your stored data is lost and taken by the attacker.
- **Bad use of your mobile resources:** Which means that your network or mobile device can go in overload so you are unable to access your genuine services. In worse scenarios, to be used by the hacker to attach another machine or network.
- **Reputation loss:** In case your Facebook account or business email account is hacked, the hacker can send fake messages to your friends, business partners and other contacts. This might damage your reputation.
- **Identity theft:** There can be a case of identity theft such as photo, name, address, credit card, etc. and the same can be used for a crime.

Anatomy of a Mobile Attack



- **Infecting the device**
- Infecting the device with mobile spyware is performed differently for Android and iOS devices.
- **Android:** Users are tricked to download an app from the market or from a third-party application generally by using social engineering attack. Remote infection can also be performed through a Man-in-the-Middle (MitM) attack, where an active adversary intercepts the user's mobile communications to inject the malware.
- **iOS**: iOS infection requires physical access to the mobile. Infecting the device can also be through exploiting a zero-day such as the JailbreakME exploit

- **Installing a backdoor**
- To install a backdoor requires administrator privileges by rooting Android devices and jailbreaking Apple devices.
- Despite device manufacturers placing rooting/jailbreaking detection mechanisms, mobile spyware easily bypasses them:
- **Android:** Rooting detection mechanisms do not apply to intentional rooting
- **iOS:** The jailbreaking “community” is vociferous and motivated

- **Bypassing encryption mechanisms and exfiltrating information**
- Spyware sends mobile content such as encrypted emails and messages to the attacker servers in plain text.
- The spyware does not directly attack the secure container. It grabs the data at the point where the user pulls up data from the secure container in order to read it.
- At that stage, when the content is decrypted for the user's usage, the spyware takes controls of the content and sends it on.


Surveillance
Audio
Camera
Call logs
Location
SMS messages
Impersonation
SMS redirection
Sending email messages
Posting to social media
Data Theft
Account details
Contacts
Call logs
Phone number
Stealing data via app vulnerabilities
Stealing international mobile equipment identity number (IMEI)
Financial
Sending premium rate SMS messages
Stealing transaction authentication numbers (TANs)
Extortion via ransomware
Phone number
Fake antivirus
Making expensive calls
Botnet activity
Launching DDoS attacks
Click fraud
Sending premium rate SMS messages

EMM Model

- The best way for an enterprise to protect their mobile technology is to implement a full lifecycle EMM solution.
- This will enforce corporate mobile security policies from initial device onboarding and protection, through monitoring and controlling the device during every day use, to its eventual retirement.
- For each phase of the mobility lifecycle, SOTI recommends a set of best practices that will improve any organizations mobile security.

ONBOARD

Before a mobile device can access company resources (e.g. networks, files, email, etc.), it is necessary to establish the identity of the user and evaluate the status of the device.

- To confirm user identity, organizations use multi-factor authentication. Multi-factor authentication is commonly achieved through an EMM solution's integration with an Identity Provider (IdP) solution.
- To assess the security posture of a mobile device, check for Jailbreak/Rooting, unapproved OS versions, malware or blacklisted apps, and failures issued by a device attestation service.

PROTECT

After the user has been verified and the integrity of the device validated, it must be secured from external threats and unauthorized disclosure of sensitive/ confidential information. You must enforce multiple layers of protection starting at the device hardware and communications networks, all the way out to the websites and apps the device employs. Failure to protect at any one of these layers could compromise the device, the confidential/sensitive information residing on it, as well as the corporate network.

MOBILE SECURITY CHECKLIST

Hardware/OS	☑ Enforce complex password policies ☑ Enforce encryption of internal storage and removable SD card(s) ☑ Disable USB access on dedicated purpose devices ☑ Update/patch OS (if supported by the device)
Apps	☑ Apply a company-branded kiosk on dedicated purpose devices to limit access to settings and apps Update/patch apps ☑ Disable side loading of apps or installation of apps from 3rd party apps stores ☑ Blacklist unapproved apps on BYOD or company-owned personally enabled (COPE) devices
Content	☑ Use an EMM email gateway for Exchange email ☑ Enforce app sharing restrictions to prevent data leakage from business apps and email accounts ☑ Use of an EMM secure document manager and secure web browser to grant secure access to corporate files and websites
Communication	☑ Disable Bluetooth pairing if not required for the device, or if unpatched Bluetooth vulnerabilities are identified ☑ Configure and enforce VPN/per-app VPN ☑ Whitelist WiFi access points on dedicated purpose devices
Cyber threats	☑ Use an EMM secure browser and block access to unapproved categories of websites (e.g. gambling websites) or websites with invalid certificates ☑ Enable/Configure antivirus protection

MONITOR

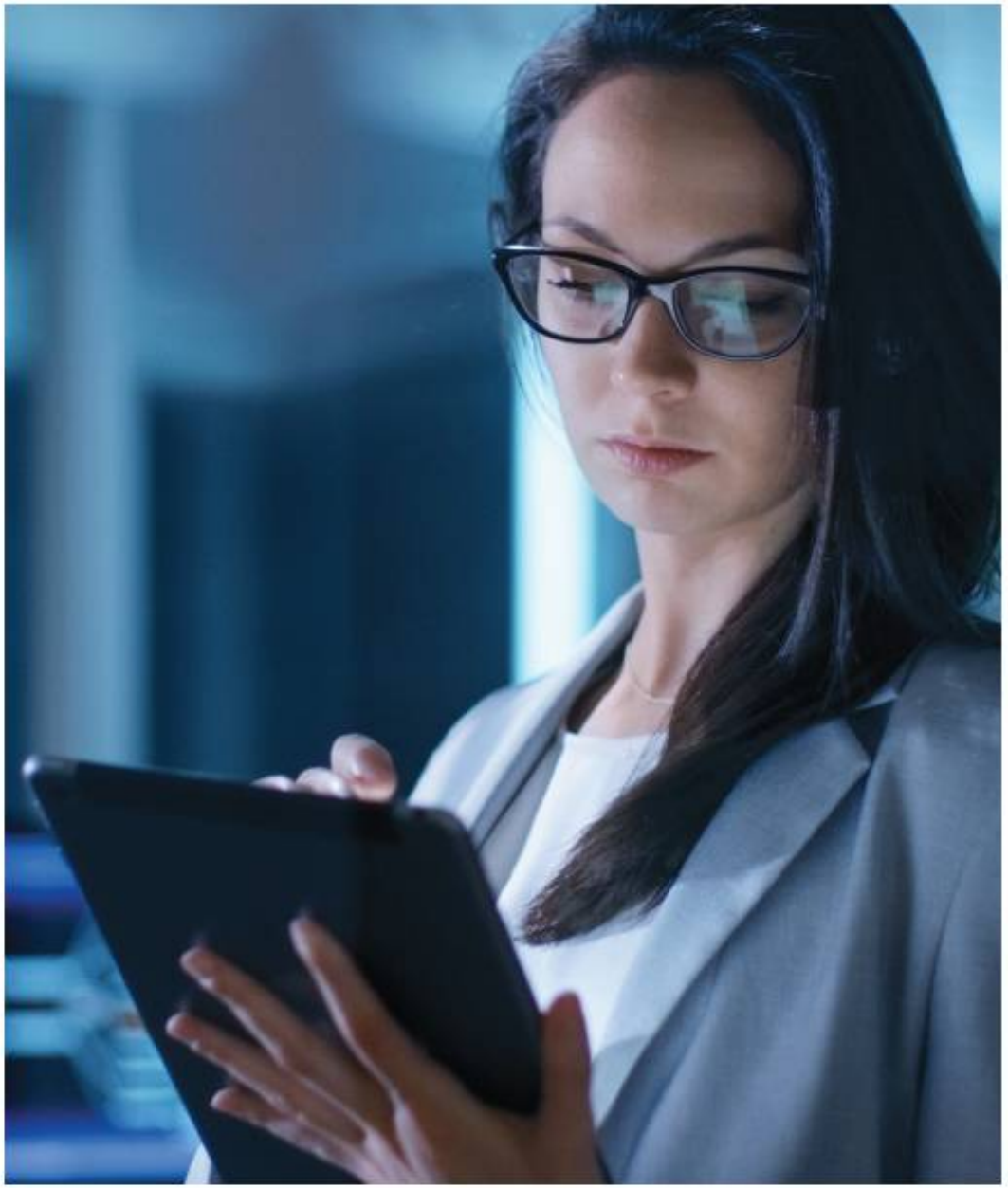
Once a device has been properly configured and protected according to company security policies, it needs to be monitored throughout its period of use to ensure its security posture is not compromised. This includes ongoing detection of PHAs and blacklisted apps, jailbreaking/rooting, and OS and apps missing key security patches. Non-compliance should result in the EMM solution taking pre-defined actions to remediate/ mitigate the impact of non-compliance.

MITIGATE

In the event the device becomes lost, stolen or compromised, an EMM solution will automatically mitigate or remediate the condition. Automated actions include:

- Lock or wipe the device, or just wipe the company apps and settings
- Send notifications to the device directly, or via email
- Block access to Exchange email
- Delete downloaded files within the EMM secure document manager
- Reconfigure the device by revoking access to company resources while continuing to enforce security settings on the device (e.g. passcode, encryption, etc.).

IT administrators can also manually initiate these mitigation and remediation actions, as required. EMM solutions typically log all interactions between management server and the device. The logs, configured policies, and diagnostic tools provided can be extremely useful in the investigation and remediation of security issues.



RETIRE

Retiring a mobile device is a critical, often overlooked phase that revokes access to company resources when a device is no longer used for work purposes, or is re-purposed for a different assignment/employee. The approach an organization takes will differ based on the scenario and the type of device being retired:

- For BYOD devices, organizations should perform a selective wipe to remove the work management profile, settings, email accounts and apps. This process leaves personal information and apps on the device untouched.
- For company-owned devices that will be recycled to a new user/assignment, organizations should perform an enterprise wipe. An enterprise wipe erases all data on the device while retaining EMM management – devices must support persistent storage or be registered to an enrollment service such as, Apple DEP, to support an enterprise wipe.
- For company-owned devices that are being de-commissioned, being fixed, or have been permanently lost/stolen, organizations should perform a full device wipe.

THANK YOU