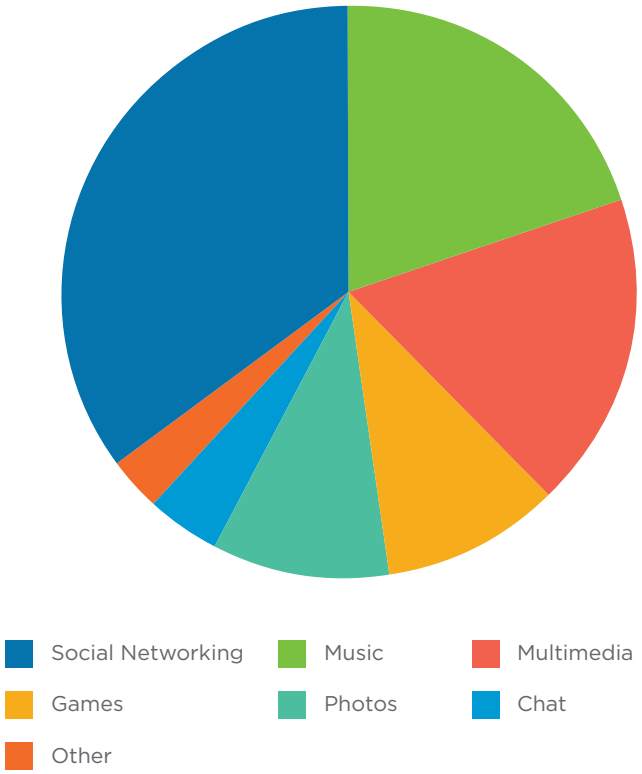
MORE MOBILE DEVICES AND APPS

Over the last decade, the growth of mobile technology has been incredible. Over two-thirds of the global population, around 5 billion people, use a mobile device. About half of mobile device users are using a smartphone, and for many people, their mobile device is their only connection to the internet. Mobile devices account for over half of the global internet traffic and this share could grow to as high as two-thirds by 2022.

What is everyone doing with their smartphone? The short answer is apps, apps and more apps. In 2017, global app downloads exceeded 175 billion (remember only 2.5 billion smartphone users). The average user has more than 80 apps on their smartphone and uses close to 40 each month. Social networking, music, multimedia and games are the most popular categories of smartphone apps.

POPULAR APP CATEGORIES



Globally, over
5 billion people
use a mobile device.

https://www.slideshare.net/wearesocialsg/global-digital-statshot-q2-2017?
https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
https://www.forrester.com/report/Forrester+Data+Mobile+Smartphone+And+Tablet+Forecast+2017+To+2022+Global/-/E-RES138971
https://www.appannie.com/en/insights/market-data/app-annie-2017-retrospective/

MORE ENTERPRISE MOBILITY

Different companies in different industries have unique mobility strategies, but their motivations for enterprise mobility is consistent — streamlining operations, increasing employee and customer satisfaction, as well as reducing costs. This is driving broader and deeper business mobility deployments — more devices used for more critical functions within the business. This technology enablement is creating a new generation of "mobile workers," beyond the classical road warriors to include executives, field workers and the growing number of telecommuters. By 2020, experts predict that almost 3/4 of the U.S workforce will be mobile workers.

The benefits of a mobile workforce are straightforward:

- 91% of remote workers feel they are more productive and happier.
- Remote workers work an additional five hours per week adding more than 250 hours of work every year.
- Teleworkers continue to work when they are sick and do not come to the office to potentially infect their coworkers.
- Companies can reduce their expenditures on real estate and office operations.

By 2020, almost 3/4 of the U.S workforce will be mobile workers.

https://getvoip.com/blog/2017/10/19/embrace-enterprise-mobility/
https://www.businesswire.com/news/home/20150623005073/en/IDC-Forecasts-U.S.-Mobile-Worker-Population-Surpass
https://cdn2.hubspot.net/hubfs/443262/TINYpulse_What_Leaders_Need_to_Know_About_Remote_Workers.pdf?t=1462203875281
http://globalworkplaceanalytics.com/resources/costs-benefits
https://www.forbes.com/sites/jeannemeister/2013/04/01/flexible-workspaces-another-workplace-perk-or-a-must-have-to-attract-top-talent/

SOTI

REQUIRES MORE MOBILE SECURITY

The downside of all the new mobile technology in the enterprise is the increased security risk. Because mobile security has not always been top-of-mind, more mobile devices and apps mean increased vulnerability. The growing pool of poorly secured devices has become an attractive targets for cyber criminals.

- Globally there has been a steady increase in the number of mobile malware infections. Total mobile malware grew 56% over the last four quarters to 21 million samples.
- In 2017, Android devices accounted for 68.5% of mobile malware infections, followed by Windows/PC devices at 27.96% and iOS only 3.5%.
- 20% of companies believe that their company has already experienced a mobile security breach, while 24% don't know if they have or haven't been breached.
- Since late 2015, the number of vulnerability scans directed at IoT devices has increased by almost 500%.

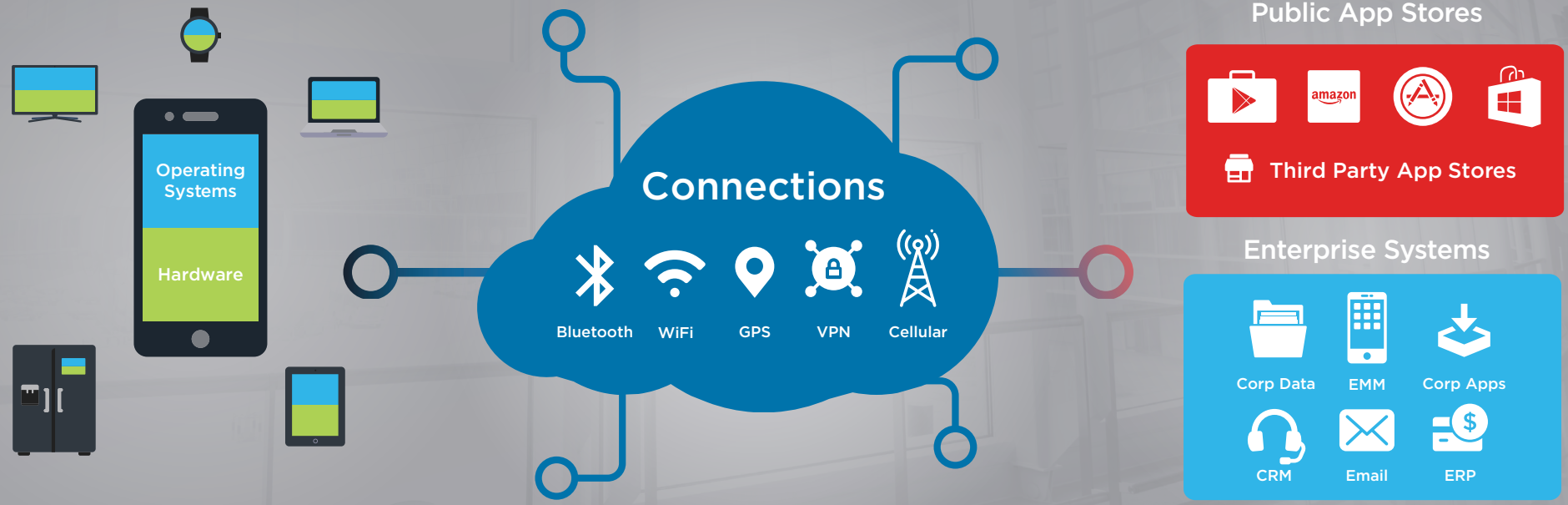
20% of companies that their company has already experienced a mobile security breach.

https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-dec-2017.pdf
https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
https://www.business.att.com/cybersecurity/archives/v2/iot/

SOTI

OVERVIEW OF COMMON MOBILE SECURITY THREATS

There are different security threats in different parts of the mobility landscape. Some target the physical device at the hardware or operating system level, while others use mobile apps and public app stores to gain a foothold on the device and from there the corporate network. Another area under threat are communication networks such as WiFi, cellular or Bluetooth. How a device is deployed (BYOD, COPE, COBO, COSU) or how it is used can create its own set of challenges. Plus, there is a growing danger from fraudulent websites and emails that prey on human nature to access sensitive company resources. What are the most common mobile threats and what are the EMM best practices to prevent or mitigate them?



SOTI

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).

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.

https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data

JAILBREAKING / ROOTING

Some users want to bypass the security of the Apple App Store or Google Play Store to install third-party apps. They do this 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:

- 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.

https://www.lookout.com/info/spectrum-of-mobile-risk-report-lp

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.

https://www.ipass.com/wifi-growth-map/index.html
https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/
https://boingboing.net/2017/03/29/democratizing-crime.html
https://www.scmagazineuk.com/billions-of-bluetooth-devices-vulnerable-to-mitm-attacks-no-user-action/article/688067/

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.

https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-dec-2017.pdf
https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/
https://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largest-malware-campaign-found-google-play/

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.

https://phishme.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf
https://techbeacon.com/sites/default/files/gated_asset/2016-cybersecurity-trend-report-ubm-ponemon-hpe-study-report-survey.pdf

SOTI

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.

https://www6.gemalto.com/breach-level-index-2017-h1-report?utm_medium=social-media&&utm_campaign=bli-lp-report
http://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

SOTI

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

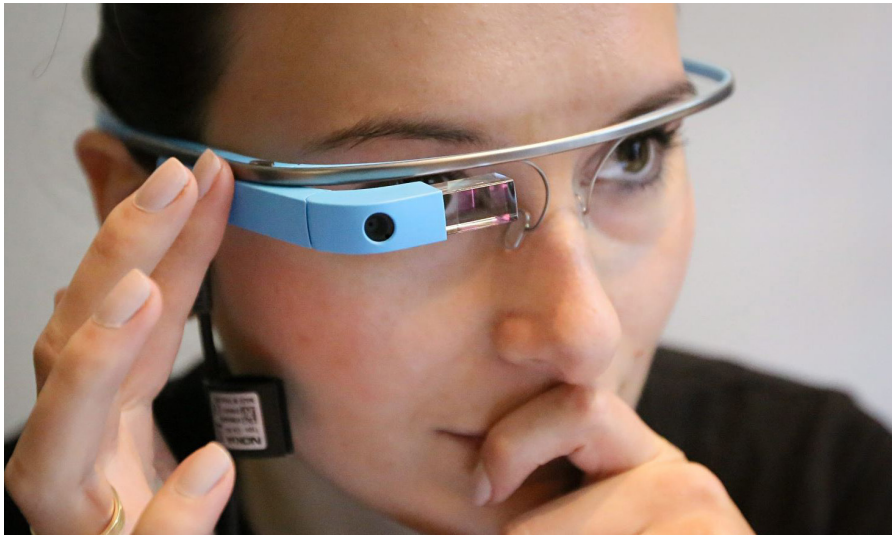
Formal BYOD Policy	Around 60% of companies have formal BYOD policies. Even in the absence of EMM, a BYOD policy can reduce many security risks.
Secure Email Gateway	Use an EMM email gateway to secure on-premise MS Exchange email and ensure email can only be accessed from managed and compliant devices.
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.

https://globenewswire.com/news-release/2016/03/22/822021/0/en/Bring-Your-Own-Device-BYOD-Market-size-worth-USD-366-95-Billion-by-2022-Global-Market-Insights-Inc.html
https://cyber-edge.com/wp-content/uploads/2017/03/CyberEdge-2017-CDR-report.pdf

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.

https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

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?

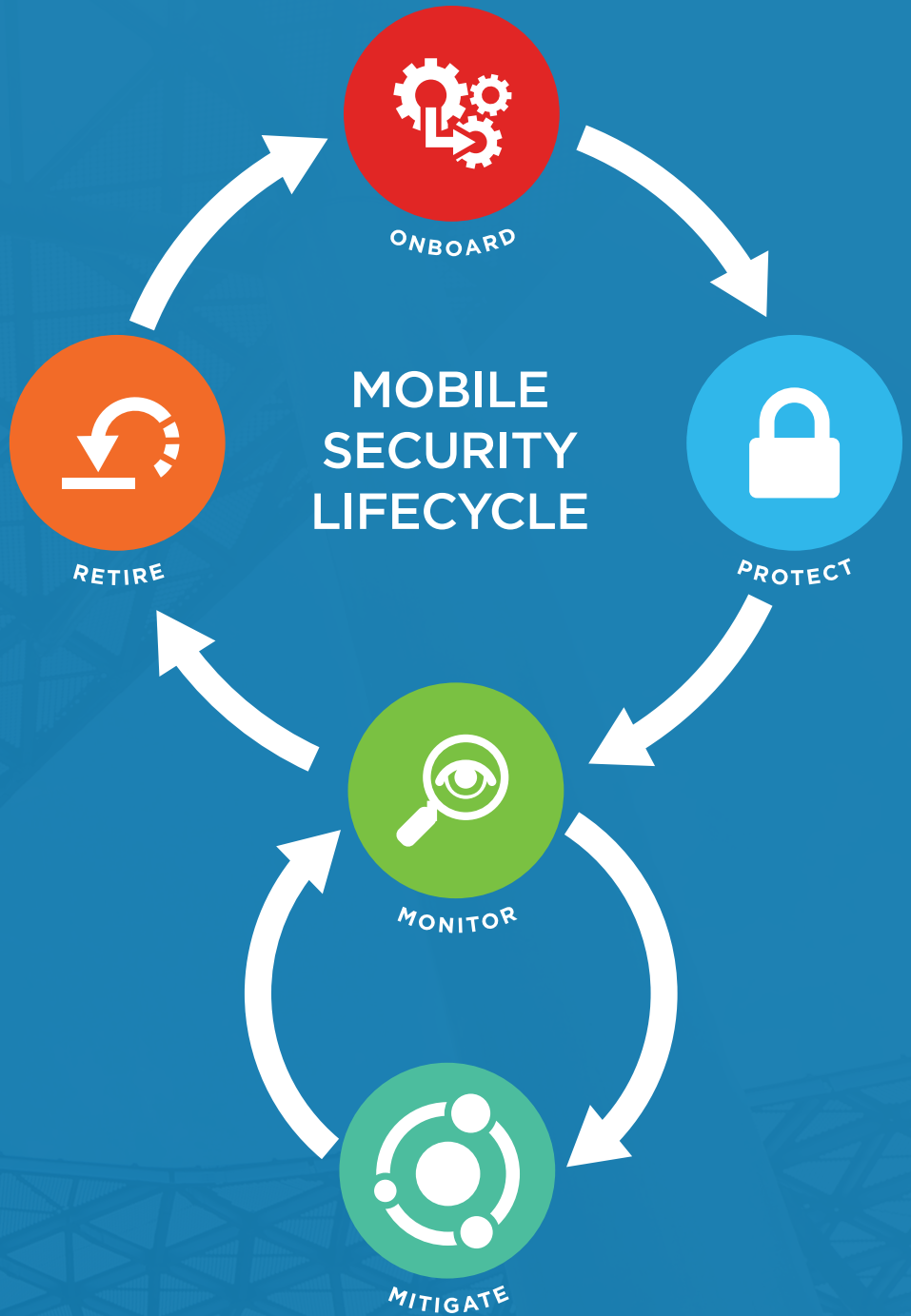
BYOD is such a big and important topic that many companies have a separate BYOD policy. Alternatively, do you only allow corporate-liable devices (COPE, COBE, CYOD), or shared devices for shift workers? How you deploy your mobile devices and what they get used for is a critical element of your corporate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

http://hosteddocs.ittoolbox.com/corporate-mobility-policy-template.pdf

USE EMM TO ENFORCE FULL LIFECYCLE MOBILE SECURITY

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.



SOTI

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, SOTI recommends that 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, SOTI recommends checking 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.