CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Cyber Threats to and from Mobile Devices

Analysis and Assessment Report

NATO CCD COE Cyber Threats Analysis and Assessment Team

October 2012

Overview

This report on Threats to and from Mobile Devices assesses the key risks, vulnerabilities and threats related to mobile device (MD), risk management issues and provides generic security recommendations and mitigation measures on the organisational and technical level. The report is primarily focused on security issues related to the management/operational level of military and civil organisations. Some elements of the report will also be of interest to the general user of mobile devices. The report material is based on information from open sources.

1. Introduction: Is a smartphone your friend or a cyber-threat?

The popularity of smartphones is clearly booming and for millions of people a mobile smartphone or mobile phone with advanced capabilities has become a valuable tool. According to an analysis from Gartner, 297 million smartphone units were sold in 2010 and 468 million units in 2011.[1] The sales only for Q2 2012 are 154 million smartphone units (OS: Android 64,1%, iOS 18,8%, Symbian 5,9%, BlackBerry 5,2%, Windows 2,7%, Bada 2,7%, and Others 0,6%).[2] The research firm Canalys has reported that during the fourth quarter of 2011 smartphone sales surpassed sales of personal computers (PCs) for the first time ever – vendors shipped 488 million smartphones in 2011 compared to 415 million client PCs.[3]

The capabilities brought by MDs can clearly be beneficial. Smartphones and personal digital assistants (PDAs) give users mobile access to email, the internet, GPS navigation and many other applications.[4] Smartphones are coming to military structures as well, for modernization of their communication systems. According to recent reports, the US Army has equipped some of its troops in Afghanistan with Google Android operated touchscreen devices. The Air Force is procuring 18,000 iPads for the purpose of virtual cockpit training for its pilots.[5]

On the other hand, a smartphone may present a threat in the hands of a hacker. At the Black Hat annual conference of hackers and security professionals in Las Vegas, two researchers showed they could unlock and start the engine of a Subaru Outback via text messages using their Android smartphone. The researchers said their technique could be used against vehicles from other automakers or, worse, similar

[1] MacDailyNews, "Gartner: Microsoft Windows Phone market share to surpass Apple's iOS in 2015", 07 April 2011. http://macdailynews.com/2011/04/07/gartner-microsoft-windows-phone-market-share-to-surpass-apples-ios-in-2015/
[2] Gartner: Global Mobile Sales Down 2%, Smartphones Surge 43%, Apple Stalls As Fans Hold Out For New iPhone, August 2012 http://techcrunch.com/2012/08/14/gartner-global-mobile-sales-down-2-smartphones-surge-43-apple-stalls-as-fans-hold-out-for-new-iphone/
[3] Canalys Press Release 2012/021, "Smart phones overtake client PCs in 2011", 03 February 2012. http://www.canalys.com/static/press_release/2012/canalys-press-release-030212-smart-phones-overtake-client-pcs-2011_0.pdf
[4] US-CERT. Paul Ruggiero and Jon Foote. "Cyber Threats to Mobile Phones". http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf
[5] Richard de Silva. "U.S. Army gets smart (phones)", 31 May 2012. http://www.defenceiq.com/defence-technology/articles/us-army-gets-smart-phones/

systems that use input from wireless signals to control items such as traffic lights, security cameras and perhaps even power grids.[6]

Further, with the increase in numbers and advancing capabilities of smartphones, they are becoming more and more valuable as targets for cyber attacks. According to some recent surveys, more than a third of information security professionals believe that mobile computing presents the biggest security threat to their organisations today and for the near future (social networks and cloud computing represent the next areas of highest security concern). This is a major issue because of the vulnerabilities that can threaten mobile computing, such as unsecured Wi-Fi access, lost or stolen devices, and malware attacks on mobile operating systems, coupled with the growing popularity of "Bring Your Own Device" (BYOD) arrangements.[7] The following report is intended to increase awareness regarding main cyber security issues related to smartphones, Mini-notebooks, PDAs and tablet devices (further referred to as "mobile devices") – the threats and vulnerabilities both to these devices and deriving from them.

2. Terminology

For the purposes of this report, the following terms are utilised:

Mobile Device - a small, portable hand-held computing device, typically with mobile phone (3G/4G/CDMA) functionality, and computing capabilities (having an operating system (OS), running various types of application software, equipped with Wi-Fi and Bluetooth), i.e. personal or corporate smartphones, personal digital assistants, miniature notebooks and tablet computers. Note that the personal/corporate distinction blurs when a personal device is officially used in an organisational working environment (Bring Your Own Device – BYOD – arrangement).
Threat – a potential circumstance or event with the possibility to cause harm. A threat can be understood as a potential attack, accident or error, but this report will focus on those related to malicious activity.
Potential threat – emerging threat based more on theoretical assumptions than real cyber incidents that have taken place.
Risk – an uncertain event or condition that, if it occurs, may have an impact on information assurance, business objectives or activities.
Risk assessment – the process of analysing the risk that potential threats and vulnerabilities pose to an information system or business process (both the probability and potential impact).
Security incident - the event when a threat and vulnerability exist at the same time and protective measures are either not implemented or not successful against a specific cyber attack.
Vulnerability – a weakness that makes a threat possible and which allows an attacker to reduce a system's information assurance.

3. Analysis and Assessment

In recent years the typical mobile personal communication device (i.e. mobile phone) has become a smartphone that is essentially a mobile personal computer (PC). This device is technologically even more developed and has even more technical possibilities than a usual PC. The main difference in workplace security is that protection of a PC at work is often a battle between attacker and IT security expert, whereas protection of a mobile device is often a fight between two quite unequal opponents – attacker and end-

[6] Fred Meier. "Hackers steal Subaru Outback with smartphone", USA TODAY, 07 August 2011.
http://content.usatoday.com/communities/driveon/post/2011/08/hackers-show-you-could-steal-a-subaru-with-your-smart-phone-black-hat-unlock-start/1
[7] FishNet Security. "Survey Shows Mobile Computing Is Top Security Concern", 11 April 2012.
http://www.fishnetsecurity.com/News-Release/Survey-Shows-Mobile-Computing-Is-Top-Security-Concern,
http://fishnetsecurity.com/6labs/Security-and-Data-Breach-Trends-2012

user. Protection of mobile devices (including BYOD) requires the same security measures as for an office PC – antivirus, local firewall, updates/patches and basic secure configuration/setup.

3.1. Risks related to mobile devices

Risks, vulnerabilities and threats in the cyber security context present a system of interconnected elements. Consequently a risk related to a security incident is defined as a function of three components – threat, vulnerability and impact**.** Following an analytical risk management approach it is reasonable to conduct a complex analysis and to look at each element of this system.

This risk assessment element as a step in the risk management procedure identifies, prioritises and estimates risk to an organisation's operations, assets, individuals and other interconnected organisations. Risk related to a security incident includes both the probability of a security incident (caused by threat at the presence of vulnerabilities) and the loss or impact caused by that incident.

A single risk may require the presence of multiple vulnerabilities and, vice versa, a single vulnerability may be the reason for different risks. One must distinguish between a threat to a MD and a threat derived from using a MD, in particular a hacked device, as a tool to attack another system. In the latter case, the loss can be considerably larger than just damage to a single mobile device. The probability of risk from MDs is also relatively high due to the large (and rapidly increasing) number of devices. Various information sources list a number of different risks related to MDs. However, the most risky areas regarding mobile devices are related to physical security, operating systems and applications.

3.1.1 Physical security risks

Breaches of physical security, especially loss or theft of a mobile device, present one of the largest risks. Loss of or leaving unattended a mobile device may result in compromise of sensitive data or the introduction of malicious code. According to surveys among IT and IT security practitioners in the United States, the top root cause of security breaches is employees' loss of mobile data-bearing devices. This risk related to human factor or organisations security drawbacks poses a very real threat to an organisation's sensitive and confidential information.[8]

3.1.2 Operating system risks

Currently the top mobile operating systems, by market share, are Android, Symbian, Apple iOS, RIM BlackBerry, Bada and Windows Phone. As of April 2012, mobile data usage shows 63.2% of mobile data traffic to be from iOS, 19.3% from Android, 2.2% from Symbian, and 2.0% from Blackberry.[9] Each operating system has distinct strengths and weaknesses, and most vendors periodically provide updates to patch identified vulnerabilities to mitigate some operating system risks. As with PCs, maintaining the most recent patches is an important security measure. It should be noted that "jailbreaking" a mobile device (bypassing vendor restrictions or limitations to gain root access) – a practice most common with iOS – may open additional vulnerabilities, in addition to preventing access to vendor patches and updates.

3.1.3 Applications risks

The number of applications (apps) available is increasing day by day, especially for the open platforms like Android. Users who download apps from untrusted sources may be downloading compromised apps infected by malware (as an example - fake antivirus applications). Unofficial third-party stores that provide alternative sources for apps are particularly dangerous. The main problem related to alternative app stores is that they are not sufficiently controlled, or may even be managed by cyber criminals, and may contain malicious apps or provide fake copies of legitimate apps, modified to realise fraud.[10] Attackers often exploit

[8] Samuel Greengard, "Employees Cause Many Data Breaches", 21 March 2012. http://www.baselinemag.com/c/a/Security/Employees-Cause-Many-Data-Breaches-576390/

[9] Gartner, Inc., "Gartner Smart Phone Marketshare 2011 Q3", 15 November 2011. http://www.gartner.com/it/page.jsp?id=1848514

[10] Pierluigi Paganini, " Cyber threats in mobile environment", 20 April 2012. http://securityaffairs.co/wordpress/4560/cyber-crime/cyber-threats-in-mobile-environment.html

security vulnerabilities in legitimate mobile apps, turning them into malicious apps. Some malicious apps are able to control functionality related to emails, SMS messages, GPS location and voice communications.

3.2. Vulnerabilities related to mobile devices

A report from Symantec shows that in 2011, while the total number of general computer vulnerabilities dropped by 20 percent from the previous year, mobile device vulnerabilities increased by 93 percent. Some consider 2011 the first year that mobile malware presented a tangible threat to businesses and consumers. Android platform users are reported to be the most vulnerable to mobile threats.[11]

The first step in a risk management process is to know what kinds of vulnerabilities are present in MD. If a vulnerability is discovered by a potential attacker and the capability to attack exists (i.e. attack tools are developed), it can create a cyber threat.
Vulnerabilities are most common in:

- *operating systems and applications* (for example: in mobile code security if applications are tested as secure only for some platforms);
- *wireless networks* (for example misuse of MD as a phone (false and malicious use of calls and SMS) through wireless GSM 3G/4G or CDMA phone link or use of MD as a computer to hack corporate LAN/WAN through Wi-Fi and Bluetooth wireless links);
- *supporting infrastructure HW/SW* (for example in GSM Service Provider's HW/SW when voice is encrypted during over-the-air transmission but subsequently decrypted within the Service Provider's network).

During the risk assessment process the following kinds of vulnerabilities have to be considered as well:

- *vulnerabilities deriving from mobile device users* (for example: MD is lost, vulnerabilities exploited through social engineering, etc.);
- *vulnerabilities deriving from organisations* (for example: when organisation doesn't possess appropriate MD usage policy or there aren't legal agreements with employees regarding MD usage, etc.);
- *vulnerabilities related to networks (LAN, Internet, GSM/CDMA).* This case is valid when there are threats from mobile devices. Vulnerabilities can be present in LAN, Internet or 3G/4G/CDMA if specific measures are not implemented, such as Network Access Control for MDs, centralized MD security checking system, centralized anti-malware for MDs, control system over new installations and previously installed applications on MDs.

The multitude of vulnerabilities (as well as the potential payoff) makes the MD very attractive to hackers. Further, there is certainly potential for the MD to be used as a vector for advanced persistent threats (APT)[12] – whether for surveillance, infiltration and/or data exfiltration – especially if a dedicated adversary were to undertake development of significant new specific exploits.

3.3. Threats to mobile devices

The second step in a risk management process is to clarify all possible cyber threats related to mobile devices.

3.3.1. Malicious applications

A recent study from ABI Research has found that mobile malware continues to rise at a staggering rate, with unique variants growing by a huge 2180% reaching a total of 17,439 strains between Q1 2011 and Q2

[11] C.J. Arlotta, "Symantec: Mobile Vulnerabilities Increase by 93% in 2011",1 May 2012. http://www.mspmentor.net/2012/05/01/symantec-mobile-vulnerabilities-increase-by-93-in-2011/
[12] Advanced Persistent Threats (APT) are computer attacks usually driven by government agencies or terrorist organizations conducting espionage or trying to take valuable data for non-financial purposes. https://www.imperva.com/resources/glossary/glossary.html

2012.[13] The vast majority of the malware samples consisted of spyware, collecting and transmitting a variety of data unbeknownst to the user, and SMS Trojans, which clandestinely transmit SMS messages (often to premium rate numbers for financial gain). **Possible risks:** infected MDs can perform actions not wanted and not known by the user, including the collection and transmission of sensitive information from a secure local network, from local Wi-Fi through 3G/4G to a hacker/attacker.

3.3.2. Threats in wireless connections (GSM or CDMA, Wi-Fi, or Bluetooth connections)

Juniper Networks describes two prominent threats related to data network communications that have emerged: Wi-Fi hacking and Man-in-the-Middle (MITM) attacks.[14] Public Wi-Fi hotspots represent a very easy channel for hackers to exploit. With the growing adoption of Wi-Fi-enabled devices, the number of Wi-Fi hotspots globally is expected to grow from 1.3 million in 2011 to 5.8 million by 2015. With readily available "sniffing" tools, finding users on a Wi-Fi network, hijacking the user's credentials, and using those credentials to impersonate the user online is now simply a matter of clicking on an icon. Attackers can quickly steal passwords, leading to financial consequences and, in many cases, identity theft.

Ralf-Philipp Weinmann, a cryptologist at the University of Luxembourg Laboratory of Cryptology and Security, has demonstrated a new attack surface via the GSM interface of mobile phones. His research shows that there are many vulnerabilities in GSM baseband codebases, and hackers equipped with inexpensive radio hardware and open source software can surreptitiously compromise a mobile phone, listen to conversations and intercept data, generate revenue via unwanted calls/SMSs/Internet activities.[15] **Possible risks**: Wireless connections, especially free/unsecured Wi-Fi networks, are channels for hackers to collect, steal and exploit information. This kind of attack also introduces the opportunity to activate exploits with user rights for further hacking (e.g. to achieve admin-rights).

3.3.3 Man-in-the-Middle Attacks (MITM)

False connection points to Communication Service Provider (CSP) networks represent a popular tactic. Wi-Fi networks are susceptible to MITM attacks as well. When executing a MITM attack, hackers insert themselves into the communication stream between a mobile device and an unsecure Wi-Fi network, logging the information relayed between entities. Given that many mobile devices submit communications in clear text, these attacks can provide the attacker access to a wide range of sensitive user and corporate information and to monitoring of conversations while using the phone. As with Wi-Fi hacking, MITM attack tools are widely available online and the methodologies are well-documented. **Possible risks**: compromise of sensitive data or identity theft widely used to perform false/changed money transfers in bank transactions and leading to possible financial consequences.

3.3.4 Direct Attacks

Direct attacks consist of an attacking system or user performing actions to exploit mobile device systems, components or interfaces. Common direct attack methods include:

- sending malicious content or packets to device interfaces;
- sending malicious and malformed messages via SMS, MMS or email;
- attacking device interface apps with malicious content or packets;
- phishing attacks via email, voice calls (so called "vishing") or SMS/MMS messages ("smishing"),
- attacking vulnerabilities or misusing capabilities within a device's browser (mobile device browser could be used to activate exploits).

---

[13] Kerry Butters, "Mobile Malware Continues to Rise", September 2012. http://security.onestopclick.com/technology_news/mobile-malware-continues-to-rise_327.htm

[14] Juniper Networks, "2011 Mobile Threats Report", February 2012, http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf

[15] Alan Brandon, "Researcher demonstrates vulnerabilities of mobile phones", 23 December 2010. http://www.gizmag.com/researcher-demonstrates-vulnerabilities-of-mobile-phones/17366/

3.3.5 Other types of threats or possibilities for infecting mobile devices:

- "attaging"(@tag) with "quick response barcodes" (QR Codes)[16], in which the scanned code directs a mobile device's browser to a malicious website;
- threats through thumb-drives/removable media (USB memory/drives, SSD, CD, DVD);
- browser-based "drive-by" attacks, in which visiting an infected website triggers an automatic malware download;
- threats through non-secure Internet surfing, emailing, Peer-to-Peer (P2P) services (instant messaging/online chat, Voice Over IP (VoIP), malicious/not observable information/links/files uploads and downloads);
- transfer/storage of infected video and photography;
- threats through social networking (Twitter, Facebook, social exploits - fake installers);
- switch on microphone and/or camera mode while the phone is inactive and transmit this information, making unwanted calls or sending unwanted SMS/MMS;
- GPS tracking, i.e. finding the position of the mobile phone (through cellular network).

3.4. Threats from mobile devices

When there are cyber threats to mobile devices and simultaneously appropriate vulnerabilities, the chance of hacking MD and to use this MD for further malicious activities becomes very high. Then we have a probability of potential cyber threats *from* mobile devices. This kind of cyber threat has to be evaluated in a risk management process as well. As MD can be used similarly to a desktop PC, the threats to a network to which it is connected are the same as from the desktop. Nevertheless analysis and assessment of cyber threats from MD presents the most interesting cases and at present is a less researched area in comparison with cyber threats to MD.

3.4.1. Threats from applications and possibilities to hack office/military networks using mobile devices

The details depend on the hacking tools available for the MD. For example, Android Network Toolkit, intended for penetration testing but more widely applicable, offers a Wi-Fi-scanning tool for finding open networks and showing all potential target devices on those networks, as well as trace route software that can reveal the IP addresses of remote servers. When a target is identified, the app offers up a simple menu with commands like "Man-In-The-Middle" to eavesdrop on local devices, or even "Attack". The app is designed to run known exploits, using vulnerabilities in non-upgraded/unpatched MD software to compromise targets.[17] **Possible risks**: a variety of malicious activity within corporate Intranet and public Internet networks.

3.4.2. BYOD and incorrect usage of mobile devices

According to Cisco Systems' annual Visual Networking Index Forecast, by 2015 there will be almost 15 billion network-connected devices, including smartphones, notebooks, tablets and other smart machines. It will likely be difficult for many companies to avoid BYOD arrangements due to the economic motivation for the company and convenience for employees. This will result in rapid growth of wireless LAN (WLAN) access points, with the need to secure this access.[18] A study of smartphone users by AVG Technologies and Ponemon Institute confirms that many people are careless in the storage and handling of sensitive information on their personal MD, leading to information leaks.[19] This threat is difficult to face, because it concerns personal devices, and it is aggravated by the behaviour of people who do not take smartphone

[16] Thomas Shaw, " 'Attaging' with QR Codes – The security threat for mobile recruitment", 04 October 2011. http://www.recruitmentdirectory.com.au/Blog/attaging-with-qr-codes-the-security-threat-for-mobile-recruitment-a439.html

[17] Andy Greenberg, "Android App Turns Smartphones Into Mobile Hacking Machines", Forbes, 8 May 2011. http://www.forbes.com/sites/andygreenberg/2011/08/05/android-app-turns-smartphones-into-mobile-hacking-machines/

[18] Jeffrey Burt, "BYOD Trend Pressures Corporate Networks", 05 September 2011. http://www.eweek.com/c/a/Mobile-and-Wireless/BYOD-Trend-Puts-Pressure-on-Corporate-Networks-186705/

[19] "The Human Factor in Data Protection, Ponemon Institute© Research Report", Sponsored by Trend Micro, conducted by Ponemon Institute LLC; January 2012. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf

security risks seriously. The risk to confidentiality is also increased due to the high probability of loss of a personal device or leaving it accessible for strangers. **Possible risks**: uncontrolled access points from BYOD-MDs can be tools and reasons for data breach from LANs.

3.4.3. Threats from uncontrolled access points

MD can create and exploit app level access points to local networks that are difficult to control. Left unmanaged, they can potentially result in a data breach. Content filtering of data going out to MD can decrease the threat considerably, and respective tools exist, e.g. ActiveSync Protector.[20] Access control by verifying that the user and the device match and applying a whitelist of allowed users should be mandatory, if mobile devices are allowed to access a local network. **Possible risks**: additional attacking points to LANs.

3.4.4. Threats from social networking

Smartphones are primarily intended for communication between persons, i.e. they are especially easy to use for social networking, but they may create a considerable threat if they also have access to a local network. Numerous mobile device apps are used to link with virtual communities for the purpose of sharing information or media. In some cases these social networks are native to MDs, often focusing on location-based information. The user of a mobile device that has access to a local network, even without any malware installed on the device, may be lured to leak data from the local network via social networking. **Possible risks**: social engineering, inadvertent disclosure of location data, possibilities to upload/download malicious links/files, the leakage of sensitive information.

3.4.5. Threat when mobile devices are used in botnets

As popular botnets are becoming smaller (a most useful botnet size today is about 10000 bots, with several botnets possibly engaged in an attack) and command and control is often performed over HTTP instead of IRC, mobile devices are becoming perfect devices for hosting bots. A new bot tool for Android has been detected by Kaspersky Lab, which also comes with a root exploit and an SMS Trojan, providing an attacker with a path to gain full control of the infected device.[21, 22] **Possible risks**: use of the mobile device to unknowingly participate in Distributed Denial-of-Service attacks, transmission of spam, infection of other devices, difficulty in attack attribution, other threats common to botnets.

3.4.6. Advanced Persistent Threats (APT)

Provided that certain basic vulnerabilities were present, a malicious or malware-infected user (insider) could exfiltrate data from data networks not connected to the Internet, using a mobile device. If a Wi-Fi, Bluetooth or wired connection to that network were knowingly or unknowingly enabled, the mobile device could connect to the network, collect data and store it for later download or transmission via GSM/CDMA. For most enterprises, concerned with advanced persistent threats, tying together operational analysis and analytics so that it includes endpoint status, information and the ability to interact with endpoint systems in real time, the ability to provide a closed detection/response ecosystem becomes a fundamental issue.[23] **Possible risk**: exfiltration of data from secure networks not connected to the Internet.

4. Conclusions and Recommendations

In the last few years rapid changes have taken place in cyber space. In some situations, IT security and cyber security have become perimeter-less, with the new “perimeter” being Identity Management, mainly because of large-scale use of mobile devices, wireless connectivity, cloud computing, Peer to Peer (P2P)

[20] ActiveSync Protector. http://www.agatsolutions.com/AgatSite/AG_Security_Suite/AG_ActiveSync_Filter.aspx
[21] Ron Condon, “Surveying the landscape of today’s mobile device security risks”, 14 March 2012. http://searchsecurity.techtarget.co.uk/news/2240146347/Surveying-the-landscape-of-todays-mobile-device-security-risks (Accessible upon subscription).
[22] US-CERT. “Defending Cell Phones and PDAs Against Attack”, 9 August 2006. http://www.us-cert.gov/cas/tips/ST06-007.html
[23] IBM Security Systems, IBM X-Force 2011 Trend and Risk Report, https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli_Organic&S_PKG=xforce-trend-risk-report (Accessible upon subscription).

connectivity and social networks. Despite the fact that employee-owned MDs in the workplace offer cost-savings in hardware, service, and support, they present a major challenge to organisation/business security if cyber security measures are not yet in place or have not yet been developed yet.

The technical and legal frameworks surrounding mobile communications and information exchange are broad and cover information security related policies, strategies, personnel, operations, devices, contracted services, technology and data protection, etc. Today, resolving cyber security challenges is a strategic direction for interested groups across multiple sectors and at every level – ensuring adequate protection of mobile devices and services contributes to overall Information Assurance.

The use of personal mobile devices in the interests of an institution can potentially reduce costs in hardware and user training, but also leads to additional risks and IT security costs. To be rational the cost-reduction from end-user hardware/training must exceed the additional IT security costs.[24] The evaluation of risks to a device or system as a function of vulnerabilities and cyber threats can lead to corresponding changes in IT Security/Cyber Security on organisational, technical and legal levels in order to protect the organisation and individual. Various information sources give a good set of security recommendations to better protect mobile devices against hacking and to protect an organisation's networks from the threats derived from hacked MDs. Some of these recommended security and mitigation measures are listed below.

4.1. The security of mobile devices on organisational level

The following organisational steps are recommended to gain and maintain control of mobile devices in working environment:

- make strategic decisions – use or not to use personal MDs in corporate work environment;
- introduce and enforce relevant policies on how MDs will be used and secured;
- decide which mobile devices (hardware, operating system) and applications best align with organisational needs and then standardise specific hardware and software;
- define what personal applications are allowed in the organisation, create policies for the use of social media in the workplace;
- analyse how sensitive corporate and personal information and other regulated information will be processed and must be secured;
- mandate immediate notification if a MD containing sensitive or confidential information is lost or stolen;
- create awareness among personnel about MD data protection activities (education, training);
- ensure sufficient funding necessary for mobile device corporate and personal data protection and security.

4.2. The security of mobile devices on technical level

Many of the recommended measures for MD are quite similar to those needed for "traditional" computers:

- installation of on-device anti-malware solutions and on-device personal firewall;
- utilisation of password protection for MD access;
- provision for the ability to separate enterprise applications and data on MDs from the employee's personal applications and data;
- usage of anti-spam software, regular MD backups and caution that applications are only downloaded from officially sanctioned sources;
- installation updates and patches of the MD OS and apps in a timely manner;
- control of remote access to MD that is inside perimeter of LAN.

[24] Nicholas G Carr, "IT doesn't matter", Harvard Business Review, May 2003. http://hbr.org/product/it-doesn-t-matter/an/R0305B-PDF-ENG (Accessible upon subscription).

4.3. The protection of organisation/business IT infrastructure against threats from mobile devices

To secure connections to corporate networks:

- implementation of network access control and appropriate access rights based on user identity and device security posture, i.e. Identity and Access Rights Management (a new perimeter to ensure secure and appropriate network access and authorisation);
- encryption of communication of corporate sensitive and confidential data (the protection of data in transit) and use of SSL VPN client for remote connection.

For corporate IT security:

- centralized administration to enforce and report on security policies across the entire MD population;
- monitoring of activity from all MDs for data leakage and/or inappropriate use, content filtering;
- centralized mobile device GSM monitoring and control (including SMS and MMS);
- centralized anti-malware for all OSs used (i.e. MD OSs must be included);
- centralized remote locate, track, lock, wipe, backup and restore functionality for MDs;
- centralized MD security checking to assess device security posture;
- centralized firewall with specific solutions to protect MD interfaces.

For mobile device management:

- control over installed apps and the installation of new apps;
- mandating the use of PINs/passcodes, as well as defining and enforcing device passcode attributes (strength, passcode expiration and so on);
- mobile device usage analysis and audits;
- the deployment of additional layers of defence that go beyond traditional perimeter defences (e.g., network firewalls and IPS) against APTs.

Further reading

"2011 Mobile Threats Report", Juniper Networks, February 2012.
http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf

"Mobile Malware Continues to Rise", Kerry Butters, September 2012.
http://security.onestopclick.com/technology_news/mobile-malware-continues-to-rise_327.htm

"Security in the Age of Mobility", TrendLabs Quarterly Security Roundup, by Trend Micro, 2012.
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_security_in_the_age_of_mobility.pdf

"Cybersecurity in the Age of Mobility: Building a Mobile Infrastructure that Promotes Productivity", Economist Intelligence Unit, Booz Allen Hamilton, 24 April 2012.
http://www.cyberhub.com/research/Mobility

"7 Tips for Upgrading IT Security", Posted by Jason Fell, 24 April 2012.
http://www.entrepreneur.com/blog/printthis/223408

"Cyber Threats to Mobile Phones", Paul Ruggiero and Jon Foote, US-CERT, 2011.
http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf

"How to protect your smartphone and tablet", The Telegraph, 26 April 2012.
http://www.telegraph.co.uk/sponsored/technology/internet-security/9214368/smartphone-and-tablet-guide.html

"How to Protect Employees' Mobile Devices From Cyber Attacks", Ivy Schmerken, 05 April 2012.
http://www.wallstreetandtech.com/data-security/232800226

"Information technology. Security techniques. Information security risk management", ISO/IEC 27005:2011.
http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742

"Making your wireless network unbreakable", Gert Hansen, 19 April 2012.
http://www.smeweb.com/index.php?option=com_content&view=article&id=3591:wirless-network-protection

"Smartphones: Information security risks, opportunities and recommendations for user", Dr. Giles Hogben and Dr. Marnix Dekker, 10 December 2010.
http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users

"Attacking with QR Codes -The security threat for mobile recruitment", Thomas Shaw, 4 October 2011.
http://www.recruitmentdirectory.com.au/Blog/attaging-with-qr-codes-the-security-threat-for-mobile-recruitment-a439.html

"Top Cyber Security Trends for 2012: #1", iMPERVA, 13 December 2011.
http://blog.imperva.com/2011/12/top-cyber-security-trends-for-2012-1.html

iMPERVA. "Hacker Intelligence Initiative, Monthly Trend Report #6", December 2011.
http://www.imperva.com/docs/HI_Security_Trends_2012.pdf