Mobile Device Security: Threats, Governance, and Safeguards

Larry G. Wlosinski,
CISSP, CAP, CCSP, CISM, CISA, CRISC, CBCP, CDP, ITIL v3
L_Wlosinski@Hotmail.com
Larry G. Wlosinski,
CISSP, CAP, CCSP, CISM, CISA, CRISC, CBCP, CDP, ITIL v3

- **Federal Government Experience** (25+ yrs.)
  - EPA, NIH, CMS, DOJ, DHS, DOE, DIA, NOAA, SSA
- **Commercial Industry Experience** (14 yrs.)
  - Insurance, International & Interstate Banking, Collections, Small Business
- **Consulting Experience**
  - Veris Group, LLC – Senior Associate
  - Computer Sciences Corp. (CSC) – Section Manager
  - Lockheed Martin – IT Security Manager
  - Booz Allen Hamilton (BAH) – Associate
  - And others – Sr. IT Security Engineer, Project Manager, etc.
- **IT Security Expertise** (16+ yrs.)
  - Cybersecurity
  - IT Security Assessments (C&A/A&A, Risk, Audit)
  - Continuity Planning (OEP, BIA, ISCP, COOP, DRP, Devolution, etc.)
  - Cloud Security
  - Policy, Procedures, Guidance, Standards, Templates, Checklists
  - Incident Response & Planning
Current State of Mobile Security
Threats
Vulnerabilities
Risks
Governance
Safeguards
Objectives

- Provide information about the current state of mobile security
- Present the treats to mobile devices
- Present the common device vulnerabilities
- Provide an understanding of the risks associated with mobile security devices
- Provide governance advice
- Provide a list of safeguards and best practices
Current State of Mobile Security

Most Commonly Used Mobile Platform
Insider Security Metrics
The Impact of Mobile Devices on Information Security: A Survey of IT Professionals
Mobile Security Incidents Are Very Expensive
BYOD Grows Quickly and Creates Problems for Organizations
State of Mobile App Security – Financial Services, Retail, Health/Medical
5 Myths About Mobile Security and Their Realities
7 Security Mistakes People Make With Their Mobile Device
Top 8 Enterprise Mobility Security Issues
Greatest Security Concerns
Which mobile operating system presents the greatest security risk?

- Android: 43%
- Apple/iOS: 36%
- BlackBerry: 22%
Insider Security Metrics

<table>
<thead>
<tr>
<th>Event</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee lost a smart phone</td>
<td>28.3%</td>
</tr>
<tr>
<td>Employee lost a laptop containing sensitive information</td>
<td>17.1%</td>
</tr>
<tr>
<td>Employee accidentally e-mailed or posted sensitive information</td>
<td>12.1%</td>
</tr>
<tr>
<td>Rogue employee inappropriately accessed sensitive documents</td>
<td>7.5%</td>
</tr>
<tr>
<td>Outside attacker compromised a server and stole data</td>
<td>2.7%</td>
</tr>
<tr>
<td>Rogue employee stole sensitive company documents</td>
<td>2.6%</td>
</tr>
<tr>
<td>IT administrator abused privileges and stole data</td>
<td>1.7%</td>
</tr>
</tbody>
</table>

Source: Forrester Consulting
Increasing numbers of mobile devices connect to corporate networks

* 93% have mobile devices connecting to their corporate networks
* 67% allow personal devices to connect to corporate networks

Customer information on mobile devices causes security concerns

* 53% report there is sensitive customer information on mobile devices, up from 47% last year (2012)
* 94% indicate lost or stolen customer information is grave concern in a mobile security incident

Mobile Security Incidents Are Very Expensive

* 79% report mobile security incidents in the past year
* 52% of large companies say cost of mobile security incidents last year exceeded $500,000
* 45% of businesses with less than 1000 employees reported mobile security incident costs exceeding $100,000
* 49% cite Android as platform with greatest perceived security risk (up from 30% last year), compared to Apple, Windows Mobile, and Blackberry
* 66% say careless employees greater security risk than cybercriminals

Among companies that allow personal devices to connect to corporate networks:

* 96% say number of personal devices connecting to corporate networks is growing
* 45% have more than five times as many personal mobile devices as they had two years ago, an increase from 36% last year
* 63% do not manage corporate information on personal devices
* 93% face challenges adopting BYOD policies
* Securing corporate information cited as greatest BYOD challenge (67%)

Arxan analysis of the top 100 paid and top 20 most popular free apps reveals that a majority have been hacked:

* 97% of top paid Android apps have been hacked
* 87% of top paid iOS apps have been hacked
* 80% of the most popular free Android apps have been hacked
* 75% of the most popular free iOS apps have been hacked

In Financial Services:

* Research has shown that hacking or malware has been the predominant method of Credit Card data breaches that occurred from 2005 to 2014
* Most apps have been hacked. The research of top financial apps reveals that:
  * 95% of Android apps have been hacked
  * 70% of iOS apps have been hacked
* The research also reveals a growing trend of financial app hacking
  * Android app hacking increased from 76% to 95%, from 2013 to 2014
  * iOS app hacking increased from 36% to 70%, from 2013 to 2014

In Retail:

* The study of top retail apps reveals that:
  * 90% of Android apps have been hacked
  * 35% of iOS apps have been hacked

In Healthcare/Medical:

* Hacks are on the rise. A separate analysis revealed that 42% of total records compromised so far in 2014 were from medical and healthcare organizations
* Similarly, our research shows that many sensitive medical/healthcare apps have been hacked – 90% of Android apps have been hacked, 22% of these apps were FDA approved apps

5 Myths About Mobile Security and Their Realities

1. Mobile devices don't store sensitive corporate data
2. Strong authentication schemes, password management controls, and device PINs are sufficient to prevent unauthorized access
3. Users are running the latest versions of iOS and Android, so they're up to date with bug fixes and other security patches.
4. Public app stores like Apple's App Store and Google's Play are safe sources, because they verify apps and block malware.
5. Secure access is not possible using public Wi-Fi network.

7 Security Mistakes People Make With Their Mobile Device

1. Failing to lock down your device
2. Not having the most up to date (and therefore the most secure) versions of your apps
3. Storing sensitive, work-related data on an unauthorized device
4. Opening questionable content
5. Not adhering to your company's social media policies
6. Not equipping employees' devices with some form of MDM or encryption
7. Using public or unsecure Wi-Fi

Top 8 Enterprise Mobility Security Issues

1. Inadequate control over lost/stolen devices
2. Users who don’t follow mobile policies
3. Rogue apps and malware
4. Poor separation of work and personal content and apps
5. Limited protection for data at rest and in transit
6. Difficulty monitoring the entire mobile fleet
7. Challenges with compliance and flexibility (meeting the needs of all users)
1. Policies that do not make business sense
2. Policies not implemented properly by mobile/endpoint IT teams
3. Policies not implemented properly by data centers, operations
4. Abuse of policies (e.g., downloading apps)
5. Device access into corporate network
6. Unknown, unauthorized, unmanaged mobile devices accessing the network
7. Data loss due to theft of mobile device (other than laptop)
8. Unauthorized data distribution from mobile device
9. Authorized devices introducing malware into network
10. Data loss due to inadvertent loss of mobile device (including laptop)
11. Data loss due to laptop theft

*CISO Executive Briefing: Building an effective Mobile Security Governance Program (7/20/11)
Threats

Mobile Device Threats
Malicious Mobile Applications
10 Trickiest Mobile Security Threats
Mobile Threats to Protect Against
Software-Based Threats
Threats from Exploitation of Vulnerable Mobile Operating System
Web-Based Threats
Network-Based Threats
Physical Threats
Mobile Device Threats to the Enterprise
User-Based Threats
Service Provider-Based Threats
High-Level Threats and Vulnerabilities
Government Mobile and Wireless Security Baseline
## Mobile Device Threats

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application-based</td>
<td>Malware</td>
</tr>
<tr>
<td></td>
<td>Spyware</td>
</tr>
<tr>
<td></td>
<td>Privacy threats</td>
</tr>
<tr>
<td></td>
<td>Vulnerable applications</td>
</tr>
<tr>
<td>Web-based</td>
<td>Phishing scams</td>
</tr>
<tr>
<td></td>
<td>Drive-by Downloads</td>
</tr>
<tr>
<td></td>
<td>Browser exploits</td>
</tr>
<tr>
<td>Network</td>
<td>Network exploits</td>
</tr>
<tr>
<td></td>
<td>Wi-Fi sniffing</td>
</tr>
<tr>
<td>Physical</td>
<td>Lost or stolen devices</td>
</tr>
</tbody>
</table>

[https://www.lookout.com/resources/know-your-mobile/what-is-a-mobile-threat](https://www.lookout.com/resources/know-your-mobile/what-is-a-mobile-threat)
1. Spyware that tracks device user activities like texting, emails, calls, location, contacts or browsing history.

2. Trojans that generate unauthorized premium rate calls, texts or purchases – all charged to the victim’s wireless bill.

3. Phishing sites that look like legitimate logins to a known service like online banking or social networks but are instead clever methods to steal user credentials.

4. Hidden Processes that run completely in the background on the user device, concealing themselves and lying in wait for certain behaviors like an online banking session to strike.

10 Trickiest Mobile Security Threats

1. Legit Mobile Apps that Mine Corporate Information
2. Hostile Enterprise-Signed Mobile Apps
3. Sophisticated Mobile Attackers
4. Non-malicious but Clueless Insiders
5. Android Fragmentation (of the operating system which includes security patches)
6. Mobile Payment Security Sources
7. Rootkits
8. Authentication Attacks
9. Connection Hijacking (i.e., Man-in-the-Middle, DNS poisoning)
10. Lack of Mobile Device Policy (to include credential storage and PII restrictions)

# Mobile Threats to Protect Against

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Man-in-the-Middle</td>
<td>Steal information and data between two parties</td>
<td>Verified encryption certificates</td>
</tr>
<tr>
<td>Unknown Infected Devices</td>
<td>Direct attacks against the network and/or device</td>
<td>Make sure that all devices in the chain of trust are secured and locked down</td>
</tr>
<tr>
<td>Rootkits</td>
<td>Provides administrative access to hackers</td>
<td>Anti-virus software, patching, and vulnerability scanning</td>
</tr>
<tr>
<td>API Key Theft</td>
<td>Homegrown systems can be exploited</td>
<td>API key management; Use APIs configured with proper security measures</td>
</tr>
<tr>
<td>Session Hijacking</td>
<td>Attacker takes over an active session and issues commands and queries</td>
<td></td>
</tr>
<tr>
<td>Human Error</td>
<td>Users not securing their device</td>
<td>Build in multiple layers of security controls; Force the use of complex passwords &amp; rotate them frequently</td>
</tr>
</tbody>
</table>
## Software-Based Threats

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Choose the hardware platform most resistant to vulnerabilities, and select an OS and specific versions most resistant to vulnerabilities.</td>
</tr>
<tr>
<td></td>
<td>Develop policies and procedures regarding the use, purchase, and installation of applications.</td>
</tr>
<tr>
<td></td>
<td>Provide user awareness training and impose security policies explicitly stating that users are forbidden to install unauthorized applications.</td>
</tr>
<tr>
<td></td>
<td>Implement firewall and signature-based malware scanners on the device.</td>
</tr>
<tr>
<td></td>
<td>Conduct pre-scheduled virus scanning</td>
</tr>
<tr>
<td></td>
<td>Use environment virtualization (i.e., sandbox) to conduct system monitoring, wiping, etc.</td>
</tr>
<tr>
<td></td>
<td>Centrally manage mobile devices to enable enterprise-wide configuration management</td>
</tr>
</tbody>
</table>
# Threats from Exploitation of Vulnerable Mobile Operating System

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploitation of Vulnerable Mobile OS</td>
<td>Configure devices securely and have the latest software patches installed</td>
</tr>
<tr>
<td></td>
<td>Establish an installation and software update schedule, and follow it</td>
</tr>
<tr>
<td></td>
<td>Enable integrity checking on the OS to detect rooting and jailbreaking</td>
</tr>
<tr>
<td>Exploitation of Vulnerable Mobile</td>
<td>Use information security policies with continuous monitoring capabilities to track mobile device assets and their security postures</td>
</tr>
<tr>
<td>Applications</td>
<td>When creating applications, programmers need to remove sensitive data properly</td>
</tr>
<tr>
<td></td>
<td>When developing secure applications for mobile devices: conduct a security assessment; check the architecture for flaws; require the use of official applications; set the appropriate level of data protection; use a key store to store sensitive identity information; and developers need to use appropriate protection when storing sensitive data.</td>
</tr>
<tr>
<td></td>
<td>Restrict software installations to only approved apps (i.e., whitelist via MDM)</td>
</tr>
<tr>
<td></td>
<td>Verify secure coding principles have been used in the development of in-house apps</td>
</tr>
</tbody>
</table>
## Web-Based Threats

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Code</td>
<td>Use same protections as threat from malware</td>
</tr>
<tr>
<td>Drive-By Downloads</td>
<td>Use certificates, tokens, or other means of signature checks</td>
</tr>
<tr>
<td>Exploitation of Vulnerable Browser</td>
<td>Allow only approved browsers on the mobile device and keep them current</td>
</tr>
<tr>
<td></td>
<td>Use strongest security settings (JavaScript, certificates, browser history, tracking, privacy policies, cookies, mobile fingerprint, direct connections, non-default browser) for the web browser.</td>
</tr>
</tbody>
</table>
## Network-Based Threats
*(Includes Wi-Fi, Cellular Bluetooth, Infrared & Near Field Communication)*

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Voice/Data Collection Over the Air</strong></td>
<td>Disable the Bluetooth, NFC, and 802.11 communications services. Also use strong network encryption and authentication techniques. Prohibit the dual-connection to multiple networks, known as “tethering” and “split-tunneling.”</td>
</tr>
<tr>
<td></td>
<td>Federal enterprises should use the 802.1x protocol for connection authentication. Also, prohibit simultaneous connections to multiple networks.</td>
</tr>
<tr>
<td><strong>Voice/Data Collection Over the Network</strong></td>
<td>Encrypt data in transit whenever possible.</td>
</tr>
<tr>
<td></td>
<td>For SMS functionality messages should be encrypted and preferably IP based</td>
</tr>
<tr>
<td><strong>Manipulation of Data in Transit</strong></td>
<td>Provide detailed instructions about high risk network situations and how they should be avoided.</td>
</tr>
<tr>
<td><strong>Manipulation of Data in Transit</strong></td>
<td>Deploy application-based encryption that has been FIPS validated.</td>
</tr>
<tr>
<td></td>
<td>Use existing remote access network capability with a VPN connection with a timeout configuration. Use 2-factor authentication and PKI certificates for device authentication and FIPS 140-2 encryption for data.</td>
</tr>
<tr>
<td></td>
<td>If there are policy restrictions about cloud features disable the features in question on the device or via MDM.</td>
</tr>
<tr>
<td></td>
<td>Conduct file verification on all executable code.</td>
</tr>
<tr>
<td></td>
<td>For out-of-band confirmation employ a desktop accessible web page, call-back to the mobile user via voice, e-mail confirmation with submitted data, etc.</td>
</tr>
<tr>
<td>Threat</td>
<td>Mitigation</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data Exposure Through RF Emission</td>
<td>To prevent private key capture use one of the following techniques: data obfuscication, leak detection (device shielding), or use both hardware and software approaches.</td>
</tr>
<tr>
<td></td>
<td>For applications that use RSA algorithms use a software obfuscication technique.</td>
</tr>
<tr>
<td>Connection to Untrusted Service</td>
<td>Use strong encryption and authentication methods for accessing D/A enterprise resources and train users to recognize when a connection has not been properly established using strong security settings.</td>
</tr>
<tr>
<td>Jamming</td>
<td>To detect Wi-Fi network jamming use an IDS/IPS and notify network administrators when detected.</td>
</tr>
<tr>
<td>Flooding</td>
<td>Limit signal penetration into the facility by using rate reduction or filtering techniques.</td>
</tr>
<tr>
<td>GPS/Geolocation</td>
<td>Disable the device’s tracking features through an MDM solution and audit the configuration regularly. Also, deploy strong encryption methods for data on mobile devices.</td>
</tr>
</tbody>
</table>
## Physical Threats

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Loss of Device</strong></td>
<td>To protect data confidentiality on lost devices: require strong encryption, establish a wipe policy and have technical capabilities in place, have a remote screen lock capability, have a policy about reporting lost or stolen devices, employ geolocation services, have a policy about protecting the device, use hardware and/or software encryption, and prohibit the disabling of data encryption.</td>
</tr>
<tr>
<td><strong>Physical Tampering</strong></td>
<td>Extend passcode policies to mobile devices. Train users on importance of physical controls and reporting suspicious instances when physical control was lost.</td>
</tr>
<tr>
<td><strong>Device-Specific Features</strong></td>
<td>Built-in cameras and microphones should be disabled or blocked when not required. To prohibit cameras from being able to take pictures and video use a shield such as opaque tape or a case cover that does not include a camera cutout. In some cases disable the camera.</td>
</tr>
<tr>
<td><strong>Supply Chain</strong></td>
<td>Acquire devices only form trusted sources and train users about information and communication technology (ICT) supply-chain threats, including counterfeit parts. For the federal government use GSA-qualified vendors and approved product lists.</td>
</tr>
<tr>
<td><strong>Mobile Peripherals</strong></td>
<td>Have a list of approved peripherals.</td>
</tr>
</tbody>
</table>
## Mobile Device Threats to the Enterprise

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to Enterprise</td>
<td>Require authenticated proxy communications to and from internal services. Require certificate-based authentication for email as well as Wi-Fi</td>
</tr>
<tr>
<td>Resources</td>
<td>Deny access to internal resources not specifically allowed to mobile users (depending on D/A policy)</td>
</tr>
<tr>
<td></td>
<td>Deploy an auditing or security information and event management (SEIM) solution</td>
</tr>
<tr>
<td></td>
<td>Document mobile device processes in an IRP.</td>
</tr>
<tr>
<td></td>
<td>For areas where sensitive information can be exposed, have visitors check their devices at the entrance and store them in a secure RF-shielded enclosure.</td>
</tr>
<tr>
<td></td>
<td>Require HSPD-12 authentication solutions. I.e., use strong authentication tied to system authorization, authentication identity management, encryption (e.g., PKI, two-factor, etc.), and IDS/IPS methods for all enterprise resource access.</td>
</tr>
<tr>
<td></td>
<td>For individuals for whom HSPD-12 does not apply, follow appropriate Federal identity management guidance (FIPS 201-2).</td>
</tr>
<tr>
<td></td>
<td>Have a certificate revocation list for authentication and use strong unlock passwords/PINs and patches to correct system vulnerabilities.</td>
</tr>
<tr>
<td></td>
<td>Use either multiple certificates for authentication or a single certificate for all authentications (e.g., system access, VPN connectivity, email access, secure web access).</td>
</tr>
</tbody>
</table>
# User-Based Threats

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Engineering</td>
<td>Train users on social engineering techniques.</td>
</tr>
<tr>
<td>Classified Information Spill</td>
<td>Develop, test, and document device cleaning procedures and train users and IT support staff on classified information spill procedures.</td>
</tr>
<tr>
<td>Incident Involving Mobile Device Features</td>
<td>Update IRPs on mobile device security.</td>
</tr>
<tr>
<td>Theft/Misuse of Services</td>
<td>Include the following in security awareness training: connecting to a hotel or Wi-Fi network, device sanitization, checking device integrity, and decommissioning a device.</td>
</tr>
<tr>
<td></td>
<td>Have the administrator both sign and encrypt configuration profiles to prevent modification or deletion of settings (Cryptographic Message Syntax, RFC 3852, is compatible with 3DES and AES 128).</td>
</tr>
<tr>
<td>Non-GFE (Employee-Owned) Devices</td>
<td>Prohibit employee-owned mobile devices purchased from unverified sources.</td>
</tr>
<tr>
<td></td>
<td>Employ password protection and data wiping capability and the ability to locate lost or stolen devices through geolocation.</td>
</tr>
<tr>
<td>Malicious Insider</td>
<td>Implement access policies that limit the use of mobile device access to enterprise resources using administrator privileges, and restrict management functions such as SSH from mobile devices.</td>
</tr>
<tr>
<td>Tracking</td>
<td>Have security policies require the use of strong encryption methods for the storage or transmission of data between the device and the MDM servers.</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Train users on social engineering techniques.</td>
</tr>
</tbody>
</table>
## Service Provider-Based Threats

<table>
<thead>
<tr>
<th>Threat</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Tracking</td>
<td><strong>No mitigation information provided.</strong></td>
</tr>
<tr>
<td>Usage Behavior Tracking via Applications</td>
<td><strong>No mitigation information provided.</strong> However, data captured will be limited to buttons dialed, GPS location, and URLs visited.</td>
</tr>
<tr>
<td>Routing/Forwarding</td>
<td>Employ encryption methods from end-to-end using FIPS 140-2 approved or IPSec/SSL tunnels. If a mobile device is not FIPS validated, do not allow any transmission or processing of sensitive data.</td>
</tr>
<tr>
<td>Data Ownership and Retention</td>
<td>The following are best practices that should be adopted:</td>
</tr>
<tr>
<td></td>
<td>(i) Treat all data channels to and from the device as insecure (e.g., IP, MMS/SMS, Voice);</td>
</tr>
<tr>
<td></td>
<td>(ii) If possible, remove all sensitive data; if not possible, encrypt the data (of each “sandbox” as a whole or on a per file basis);</td>
</tr>
<tr>
<td></td>
<td>(iii) Configure the device with non-specific identification parameters;</td>
</tr>
<tr>
<td></td>
<td>(iv) Adopt virtualization and sandbox technologies to contain sensitive data; and</td>
</tr>
<tr>
<td></td>
<td>(v) Work closely with a carrier that understands data ownership and retention issues and provides a clear policy as well as an SLA for data management and retention.</td>
</tr>
</tbody>
</table>
High-Level Threats and Vulnerabilities

- Lack of Physical Security Controls
- Use of Untrusted Mobile Devices
- Use of Untrusted Networks
- Use of Untrusted Applications
- Interaction with Other Systems
- Use of Untrusted Content
- Use of Location Services

## Government Mobile and Wireless Security Baseline

<table>
<thead>
<tr>
<th>Element</th>
<th>Threat</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Malware</td>
<td>App configuration management &amp; monitoring</td>
</tr>
<tr>
<td></td>
<td>Exploitation of vulnerable apps</td>
<td>D/A App Store, whitelisted/blacklisted apps</td>
</tr>
<tr>
<td></td>
<td>Compromised apps</td>
<td>Secure app development</td>
</tr>
<tr>
<td></td>
<td>Data/information leakage</td>
<td>App wrapping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>App vetting and certification</td>
</tr>
<tr>
<td>Devices</td>
<td>Insecure configuration</td>
<td>Device provisioning &amp; management</td>
</tr>
<tr>
<td></td>
<td>Vulnerable operating system</td>
<td>Mobile device integrity (Roots of Trust)</td>
</tr>
<tr>
<td></td>
<td>Unauthorized access</td>
<td>Device password to unlock device</td>
</tr>
<tr>
<td></td>
<td>Virus/malware</td>
<td>Whitelisted/blacklisted apps, user training</td>
</tr>
<tr>
<td></td>
<td>Loss of sensitive data</td>
<td>Encryption of data at rest (FIPS)</td>
</tr>
<tr>
<td></td>
<td>Device loss/Theft</td>
<td>Remote wipe of agency apps &amp; data</td>
</tr>
<tr>
<td>Infrastructure: Agency</td>
<td>Unauthorized access</td>
<td>PIV-based user authentication</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Virus/malware</td>
<td>Device authentication</td>
</tr>
<tr>
<td></td>
<td>Data integrity</td>
<td>Device malware scan, integrity check &amp; monitoring</td>
</tr>
<tr>
<td></td>
<td>Compromised apps</td>
<td>Signed apps &amp; app verification</td>
</tr>
<tr>
<td></td>
<td>Insecure coding</td>
<td>Mobile app development &amp; security vetting</td>
</tr>
<tr>
<td>Infrastructure: Access</td>
<td>Eavesdropping, data interception</td>
<td>Encryption of data in transit (VPN)</td>
</tr>
<tr>
<td>Networks</td>
<td>Voice/Data collection over the air</td>
<td>VPN, disable split tunneling &amp; tethering</td>
</tr>
<tr>
<td></td>
<td>Drive-by downloads</td>
<td>User training and Rules of Behavior</td>
</tr>
<tr>
<td></td>
<td>Location tracking (GPS)</td>
<td>Device configuration profile</td>
</tr>
<tr>
<td></td>
<td>Behavior tracking</td>
<td>Carrier SLA</td>
</tr>
</tbody>
</table>

Vulnerabilities

Vulnerabilities, Threats, & Risk
Why Mobile Applications are Insecure
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Threat</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information travels across wireless networks, which are often less secure than wired networks.</td>
<td>Malicious outsiders can do harm to the enterprise.</td>
<td>Information interception resulting in a breach of sensitive data, enterprise reputation, adherence to regulation, legal action.</td>
</tr>
<tr>
<td>Mobility provides users with the opportunity to leave enterprise boundaries and thereby eliminates many security controls.</td>
<td>Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this malware into the enterprise network.</td>
<td>Malware propagation, which may result in data leakage, data corruption and unavailability of necessary data</td>
</tr>
<tr>
<td>Bluetooth technology is very convenient for many users to have hands-free conversations; however, it is often left on and then is discoverable.</td>
<td>Hackers can discover the device and launch an attack.</td>
<td>Device corruption, lost data, call interception, possible exposure of sensitive information.</td>
</tr>
<tr>
<td>Unencrypted information is stored on the device.</td>
<td>In the event that a malicious outsider intercepts data in transit or steals a device, or if the employee loses the device, the data are readable and usable.</td>
<td>Exposure of sensitive data, resulting in damage to the enterprise, customers, or employees</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Threat</td>
<td>Risk</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lost data may affect employee productivity.</td>
<td>Mobile devices may be lost or stolen due to their portability. Data on these devices are not always backed up.</td>
<td>Workers dependent on mobile devices unable to work in the event of broken, lost or stolen devices and data that are not backed up.</td>
</tr>
<tr>
<td>The device has no authentication requirements applied.</td>
<td>In the event that the device is lost or stolen, outsiders can access the device and all of its data.</td>
<td>Data exposure, resulting in damage to the enterprise and liability and regulation issues.</td>
</tr>
<tr>
<td>The enterprise is not managing the device.</td>
<td>If no mobile device strategy exists, employees may choose to bring in their own, unsecured devices. While these devices may not connect to the virtual private network (VPN), they may interact with e-mail or store sensitive documents.</td>
<td>Data leakage, malware propagation, unknown data loss in the case of device loss or theft.</td>
</tr>
<tr>
<td>The device allows for installation of unsigned third-party applications.</td>
<td>Applications may carry malware that propagates Trojans or viruses; the applications may also transform the device into a gateway for malicious outsiders to enter the enterprise network.</td>
<td>Malware propagation, data leakage, intrusion on enterprise network.</td>
</tr>
</tbody>
</table>
1. The “rush to release” results in mobile apps that can have vulnerabilities.
2. Mobile apps are often tested infrequently and too late.
3. Malware-infected mobile apps and devices will increase.
4. Not enough is spent on mobile app security.
5. There is a dearth of trained and expert security professionals.
6. Organizations lack policies that provide guidance on employees’ use of mobile apps.
Risk

Risk Categories
Top 10 Mobile App Risks
OWASP Top 10 Mobile Risks
Strategies to Address Risk
Handling Regulatory Risk

IF THE CLOUD EVER DID GO DOWN, WOULD IT BE CALLED FOG?
Top 10 Mobile App Risks

1. Activity monitoring and data retrieval
   1. Messaging (Short Message Service (SMS) & E-mail)
   2. Audio (calls and open microphone recording)
   3. Video (still and full-motion)
   4. Location
   5. Contact list
   6. Call history
   7. Browsing history
   8. Input
   9. Data Files

2. Unauthorized dialing, SMS and payments

http://www.veracode.com/blog/2010/12/mobile-app-top-10-list
3. Unauthorized network connectivity (exfiltration or command & control)
   1. Email
   2. SMS
   3. HTTP GET/POST
   4. TCP socket
   5. UDP socket
   6. DNS exfiltration
   7. Bluetooth
   8. Blackberry Messenger

4. User Interface (UI) Impersonation

http://www.veracode.com/blog/2010/12/mobile-app-top-10-list
Top 10 Mobile App Risks

5. System modification (rootkit, APN proxy config)
6. Logic or Time bomb
7. Sensitive data leakage (inadvertent or side channel)
   1. Location
   2. Owner ID info: name, number, device ID
   3. Authentication credentials
   4. Authorization tokens
8. Unsafe sensitive data storage
9. Unsafe sensitive data transmission
10. Hardcoded password/keys

http://www.veracode.com/blog/2010/12/mobile-app-top-10-list
OWASP Mobile Top 10 Risks

M1 – Weak Server Side Controls
M2 – Insecure Data Storage
M3 – Insufficient Transport Layer Protection
M4 – Unintended Data Leakage
M5 – Poor Authorization and Authentication
M6 – Broken Cryptography
M7 – Client Side Injection
M8 – Security Decisions Via Untrusted Inputs
M9 – Improper Session Handling
M10 – Lack of Binary Protections
## Strategies to Address Risk

<table>
<thead>
<tr>
<th>Risk</th>
<th>Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>A lost or stolen mobile device</td>
<td><strong>Implement a central management console</strong> for device remote control—i.e., location tracking, data wipe-out, password/PIN change or strong user authentication. Ensure that mobile devices are encrypted so information is unusable in the event of loss or theft.</td>
</tr>
<tr>
<td>Providing support to various devices</td>
<td>Turn to cross-platform <strong>centrally managed mobile device managers</strong>.</td>
</tr>
<tr>
<td>Controlling data flow on multiple devices</td>
<td>Secure the systems that are accessed with <strong>authorization, encryption and privileges control</strong>.</td>
</tr>
<tr>
<td>Preventing data from being synchronized onto mobile devices</td>
<td><strong>Monitor and restrict data transfers</strong> to handheld or removable storage devices and media from a single, centralized console.</td>
</tr>
<tr>
<td>Keeping up with the usage of the latest and greatest devices</td>
<td>Create keen <strong>user awareness</strong> on information assets, risks and value to the enterprise.</td>
</tr>
<tr>
<td>Promoting accountability, responsibility and transparency with device usage</td>
<td><strong>Track the way devices are used</strong>, and provide regular feedback to management.</td>
</tr>
<tr>
<td>Demonstrating regulatory compliance</td>
<td>Implement a <strong>central management console</strong> to manage all stages of asset management, from installation to retirement.</td>
</tr>
</tbody>
</table>

---

**ISACA: Securing Mobile Devices (August 2010)**

Handling Regulatory Risk

1. Talk to legal and HR in the respective countries where BYOD devices are to be supported in order to understand local privacy and data security laws.
2. Create tiered policies per geographical segment that expand on the general BYOD policy.
3. Ensure your policy addresses the risk areas (e.g., privacy, data protection, monitoring, data breach, data ownership).
4. Ensure that local IT has the right processes in place to support the policy.
5. Review, monitor and revise policies regularly.
6. Segment business environments and data from personal employee data as much as possible.
7. Create a policy structure that is a streamlined governance workflow to address emerging risk areas, making the policy approval process faster and more agile.
Governance Program
Challenges Facing End User Device Governance
Considerations: Development, Implementation, & O&M
Mobile Device Governance Strategy Issues to Consider
Categories of Security Services to be Considered
Challenges and Barriers Facing BYOD Deployment
8 Components of a Successful BYOD Strategy
8 Steps to Secure & Improve Your BYOD Program
Sample BYOD Policy Outline
The 10 Commandments of BYOD
Top Tips to Establish a Successful Mobile Governance Plan
Managing Support for BYOD Devices
Hidden Service Costs of BYOD
Top 10 Recommendations for Mobile Security Guidelines to Improve Security of Mobile Devices
General Policy
Contents of a Mobile Security Policy
15 Mobile Policy Best Practices
Data Communication and Storage
User and Device Authentication
Application Safeguards
Cybersecurity for Electronic Devices
Defending Cell Phones and PDAs Against Attack
7 Enterprise Mobile Security Best Practices
Best Practices to Help Protect Mobile Devices
5 Steps for Achieving Effective Mobile Security Governance
Here is What iCloud Backs Up
Mobile Security Program Test
Governance Program
Challenges Facing End User Device Governance

- Proliferation of file shares: 45%
- Lack of coordinated governance: 42%
- Mobile devices: 41%
- User adoption of existing solutions: 40%
- Lack of budget and executive support: 39%
- Difficulty integrating with other repositories/new business apps: 36%
- Proliferation of unauthorized file-sharing sites: 36%
- Migrating content from old systems or storage locations: 35%
- Lack of available expertise and implementation: 29%
- Cost and implementation difficulties of ECM systems: 26%
- Cost of annual maintenance on software not deployed: 25%

Development Considerations

- Architecture
- Authentication
- Cryptography
- Configuration Requirements
- Device Provisioning
- Application Vetting and Certification Requirements
Implementation Considerations

- Connectivity
- Protection
- Authentication
- Applications
- Management
- Logging
- Performance
- Security of the Implementation
- Default Settings

Operations and Maintenance Considerations

- Check for upgrades and patches
- Synchronization of device to infrastructure clock
- Reconfiguring access control features
- Detecting and documenting anomalies
- Keeping an active inventory
- Providing training and awareness
- Revoking access to or deleting risky applications
- Scrubbing sensitive data from the mobile device

Critical Elements of a Successful Mobile Security Plan

1. Employee education
2. Endpoint or device security
3. Secure wireless connections
4. Mobile device management (MDM)
5. Enterprise infrastructure integration

Define allowable device types (enterprise-issued only vs. personal devices).

Define the nature of services accessible through the devices.

Identify the way employees use the devices, taking into account the organization’s corporate culture, as well as human factors.

Integrate all enterprise-issued devices into an asset management program.

Describe the type of authentication and encryption that must be present on devices.

Outline the tasks for which employees may use the device and the types of applications that are allowed.

Clarify how data should be securely stored and transmitted.
Categories of Security Services to be Considered

- **General policy:**
  - enforce enterprise security policies on the mobile device, such as restricting access to hardware and software
  - manage wireless network interfaces, and
  - automatically monitoring, detecting, and reporting when policy violations occur.

- **Data communication and storage:**
  - support strongly encrypted data communications and data storage
  - wipe the device before reissuing it, and
  - remotely wipe the device if it is lost or stolen and is at risk of having its data recovered by an untrusted party.
Categories of Security Services to be Considered

* **User and device authentication:**
  * require device authentication and/or other authentication before accessing organization resources
  * reset forgotten passwords remotely
  * automatically lock idle devices, and
  * remotely lock devices suspected of being left unlocked in an unsecured location.

* **Applications:**
  * restrict which app stores may be used and which applications may be installed
  * restrict the permissions assigned to each application
  * install and update applications
  * restrict the use of synchronization services
  * verify digital signatures on applications, and
  * distribute the organization’s applications from a dedicated mobile application store.
Challenges and Barriers Facing BYOD Deployment

- Mobile device security
- Data breach security
- Mobile data security
- Mobile application security
- Integration with back-end corporate systems
- Controlling employee use of apps
- Executive sponsorship
- Cost of help desk support
- Country-specific regulations
- Expense of implementing applications
- Industry-specific regulatory requirements
- ROI for BYOD
- Cost of training
- Mobile app development costs

8 Components of a Successful BYOD Strategy

1. Sustainability – Maintain a positive user experience
2. Trust Model – Mitigate security risks
3. Device Selection – It’s a popularity contest
4. Liability – Protect your company from legal action
5. User Experience and Privacy – Establish employee trust
6. Economics – The cost of doing BYOD
7. App Design and Governance - Enforce security without becoming Big Brother
8. Internal Marketing – Build your IT ‘brand’
8 Steps to Secure & Improve Your BYOD Program

1. Create a strategy for BYOD with a business case and a goal statement
2. Involve stakeholders early through the formation of a mobility group
3. Create a support and operations model
4. Analyze the risk
5. Create a BYOD policy [next slide]
6. Secure devices and apps
7. Test and verify the security of the implementation
8. Measure success, ROI and roll-forward lessons learned

Sample BYOD Policy Outline

1. General security requirements for mobile devices
2. Authentication (passcode/PIN) requirements
3. Storage/transmission encryption requirements
4. Requirements to automatically wipe devices after a number of failed login attempts
5. Usage restrictions for mobile devices
6. Company liability
7. Rights to monitor, manage and wipe
8. Support model
9. Leading practices for mobile data usage on international travel
10. Acceptable use (if different from the normal acceptable use policy)

The 10 Commandments of BYOD

1. Create thy policy before procuring technology
2. Seek flock’s devices
3. Enrollment shall be simple
4. Thou shall configure devices over-the-air
5. Give thy users self-service
6. Hold sacred personal information
7. Part the seas of corporate and personal data
8. Monitor thy flock-herd automatically
9. Monitor thy data usage
10. Drink from the fountain of ROI

Top Tips to Establish a Successful Mobile Governance Plan

- Let each employee know how the device is to be used, and establish acceptable volumes of usage.
- Confirm that your policies safeguard the security of company data and address all security concerns.
- Make clear what apps may be used by your employees and which ones are off limits.
- Share best practices and lessons learned so that all employees know how to stay in compliance.
- Make sure your policies clearly state the consequences of violating user guidelines.
- Monitor costs and usage continually – regular monitoring will result in cost savings in the long run.
- Scrutinize your policies and guidelines to keep your plan on track, and make changes when necessary.
- Consider management software that keeps tabs on your devices.

http://mobilesolutions.net/mobile-governance-plan/
1. **Create and enforce** an appropriate BYOD support and usage policy.

2. **Revamp existing support processes** to include secure provisioning and deprovisioning (wiping) of devices, and an increased level of self-help.

3. **Create a patch education process** to encourage users to update their mobile devices.

4. **Introduce a social support mechanism** to augment the existing IT support team.

5. **Implement** a wiki/knowledge base employee self-service support solution.
## Hidden Service Costs of BYO

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User device control</td>
<td>User device control means that IT departments may lose a layer of control that they have with corporate-labile devices</td>
</tr>
<tr>
<td>Users’ expectations relating to the support of BYOD</td>
<td>Managing users’ expectations relating to the support of BYOD will reduce the new support calls relating to incidents that service desks are unable to manage</td>
</tr>
<tr>
<td>Costs associated with request fulfillment</td>
<td>Identify the potential costs associated with request fulfillment following requests for paid applications to aid productivity to the service desk</td>
</tr>
<tr>
<td>Additional training of service desk staff</td>
<td>Additional training will ensure that the service desk staff are kept up to date as device operating systems are updated</td>
</tr>
</tbody>
</table>
1. Add mobile security to existing employee security awareness programs.
2. Create and implement an IT policy that governs usage and ensures employees’ understanding.
3. Perform threat modeling to identify the risks of moving applications to a mobile platform.
4. Train application developers in secure coding practices for mobile device platforms.
5. Limit the sensitive data transferred to mobile devices, or consider view-only access.
6. Utilize Mobile Device Management (MDM) software to create an encrypted password-protected sandbox for sensitive data and enforce device-side technical policies.
7. Perform technical security assessments on mobile devices and the supporting infrastructure — focus on device-side data storage.
8. Establish a program that continually evaluates new and emerging threats in mobile platforms.
9. Increase monitoring controls around mobile device connection points when feasible.
10. Assess classic threats against web-based applications and infrastructure.

Guidelines to Improve Security of Mobile Devices

- Develop system **threat models** for mobile devices and the resources that are accessed through the mobile devices.
- Consider the merits of each provided security service, determine which services are needed for their environment, and then design and acquire one or more **solutions that collectively provide** the necessary services [see next slide].
- Implement and test a **pilot** of their mobile device solution before putting the solution into production.
- Fully **secure each organization-issued mobile device** before allowing a user to access it.
- Regularly maintain **mobile device security**.
General Policy

* Restrict **user and application access to hardware**, such as the digital camera, GPS, Bluetooth interface, USB interface, and removable storage.

* Restrict **user and application access to native OS services**, such as the built-in web browser, email client, calendaring, contacts, application installation services, etc.

* Manage **wireless network interfaces** (Wi-Fi, Bluetooth, etc.)

* **Automatically** monitor, detect, and report when **policy violations** occur, such as changes from the approved security configuration baseline, and automatically take action when possible and appropriate

* Limit or prevent access to enterprise services based on the mobile device’s **operating system version** (including whether the device has been rooted/jailbroken), vendor/brand, model, or mobile device management software client version (if applicable).
Contents of a Mobile Security Policy*

- The mobile devices you will be supporting
- The level of end-user support you will provide and how to access support
- Definitions of all key terms, including mobile device and mobile device management
- Who will have access to specific data and applications?
- The data and activities that your enterprise will monitor and track, differentiating between corporate-owned and personal devices. This may include texting, email, browsing the Internet, downloads, GPS tracking, instant messaging, storage of multimedia files and more.
- A privacy policy that details what you will and will not do with the information that is monitored and tracked on both company and employee-owned devices.
- The specific actions your company will take if the end user violates company-usage policies.
- Defined defensive measures, such as remote wipes, that the company will take if the device is lost or stolen, or if the employee moves to another position within the company or is terminated.

*IBM Global Technology Services: Developing More Effective Mobile Enterprise Programs
15 Mobile Policy Best Practices

1. Engage the business to understand their mobile requirements
2. Determine the varying levels of service and support options for the segmented workforce
3. Reserve the right to manage all devices with access to corporate resources like PCs
4. Protect the integrity and privacy of corporate data by isolating it from personal data
5. Enforce strong security policies that prevent data security breaches
15 Mobile Policy Best Practices

6. Consider disabling features and user activities in heavily regulated environment
7. Extend acceptable use policies to all current and future mobile devices
8. Determine a tiered reimbursement policy for voice and data service costs
9. Proactively monitor ongoing data and voice usage and expenses
10. Determine how users will be provisioned with enterprise class applications
11. Require users to back up their own data
12. Ensure that everything that falls outside of Infrastructure & Operations (I&O) technology control is baked into Policy
13. Require users to understand and agree to an acceptable use policy
14. Address ramifications for non-compliance of corporate policies and provide examples
15. Revisit the policy at least annually
**Data Communication and Storage**

- Strongly **encrypt data communications** between the mobile device and the organization. This is most often in the form of a VPN, although it can be established through other uses of secure protocols and encryption.

- Strongly **encrypt stored data** on both built-in storage and removable media storage. Removable media can also be “bound” to particular devices such that encrypted information can only be decrypted when the removable media is attached to the device, thereby mitigating the risk of offline attacks on the media.

- **Wipe the device** (to scrub its stored data) before reissuing it to another user, retiring the device, etc.

- **Remotely wipe the device** (to scrub its stored data) if it is suspected that the device has been lost, stolen, or otherwise fallen into untrusted hands and is at risk of having its data recovered by an untrusted party.

- A device often can also be **configured to wipe** itself after a certain number of incorrect authentication attempts.
User and Device Authentication

* Require a device password/passcode and/or other authentication (e.g., token-based authentication, network-based device authentication, domain authentication) before accessing the organization’s resources. This includes basic parameters for password strength and a limit on the number of retries permitted without negative consequences (e.g., locking out the account, wiping the device).

* If device account lockout is enabled or the device password/passcode is forgotten, an administrator can reset this remotely to restore access to the device.

* Have the device automatically lock itself after it is idle for a period (e.g., 5 minutes).

* Under the direction of an administrator, remotely lock the device if it is suspected that the device has been left in an unlocked state in an unsecured location.
Application Safeguards

* Restrict which **app stores** may be used.
* Restrict which applications may be installed through **whitelisting** (preferable) or **blacklisting**.
* Restrict the **permissions** (e.g., camera access, location access) assigned to each application.
* **Install, update, and remove applications.** Safeguard the mechanisms used to perform these actions. Keep a current inventory of all applications installed on each device.
* **Restrict the use of operating system and application synchronization services** (e.g., local device synchronization, remote synchronization services and websites).
* **Verify digital signatures on applications** to ensure that only applications from trusted entities are installed on the device and that code has not been modified.
* Distribute the organization’s applications from a dedicated mobile **application store**.
Follow general guidelines for protecting portable devices

Be careful about posting your cell phone number and email address

Do not follow links sent in email or text messages

Be wary of downloadable software

Evaluate your security settings

https://www.us-cert.gov/ncas/tips/ST06-007
1. Mobile Devices Need Anti-malware Software
2. Secure Mobile Communications
3. Require Strong Authentication, Use Password Controls
4. Control Third-party Software
5. Create Separate, Secured Mobile Gateways
7. Perform Regular Mobile Security Audits, Penetration Testing

**Best Practices to Help Protect Mobile Devices**

- Maintain **up-to-date software**, including operating systems and applications;
- Install **anti-virus software** as it becomes available and maintain up-to-date signatures and engines;
- Enable the personal identification number (**PIN**) or **password** to access the mobile device, if available;
- **Encrypt personal and sensitive data**, when possible;
- **Disable features not currently in use** such as Bluetooth, infrared, or Wi-Fi;
- Set Bluetooth-enabled devices to **non-discoverable** to render them invisible to unauthenticated devices;
- **Use caution** when opening email and text message **attachments** and clicking **links**;
- Avoid opening files, clicking links, or calling numbers contained in unsolicited email or text messages;
- **Avoid joining** unknown Wi-Fi networks;
- Delete all information stored in a device prior to **discarding** it; and
- Maintain situational awareness of threats affecting mobile devices.
5 Steps for Achieving Effective Mobile Security Governance

1. Knowing Your Mobile Environment Risks
2. Developing an Effective Mobile Security Policy
3. Ensuring Employees’ Responsibility and Awareness
4. Establishing a Baseline Security Configuration
5. Building a Mobile Aware IT Infrastructure

http://www.csoonline.com/article/2123988/mobile-security/5-steps-for-achieving-effective-mobile-security-governance.html
Here is What iCloud Backs Up

- Information about purchased music, movies, TV shows, apps, and books, but not the purchased content itself
- Photos and videos in Camera Roll
- Contacts, calendar events, reminders, and notes
- Device settings
- App data
- PDFs and books added to iBooks but not purchased
- Call history
- Home screen and app organization
- iMessage, text (SMS), and MMS messages
- Ringtones
- HomeKit data
- HealthKit data
- Visual Voicemail
There are seven questions you should be able to answer:

1. How many mobile devices are connected to our network?
2. How do I know how many devices we have?
3. How are these devices connecting?
4. How often are these devices connecting?
5. What data are these devices accessing?
6. How many of these devices are managed?
7. How many comply with our corporate policies?

If organizations can’t answer these questions with speed and certainty, they may need to create a mobile security program.
Safeguards

Physical Device Locks
Biometric Device Locks
10 Tips to Prevent Mobile Malware
Tips for Malware-Free Smartphone
iPad Privacy
10 Common Mobile Security Problems to Attack
Take Steps to Protect Your Mobile Phone
How to Protect a Mobile Phone from Being Stolen
Protecting Your Tablet in Case it is Lost or Stolen
Act Quickly if Your Mobile Phone or PDA Is Stolen
How You Can Fight Back
Physical Device Locks
Biometric Device Locks
10 Tips to Prevent Mobile Malware

1. Inform users about mobile risks
2. Consider the security of over-the-air networks used to access company data
3. Establish and enforce bring-your-own-device (BYOD) policies
4. Prevent jailbreaking (i.e., removing the security limitations imposed by the operating system vendor)
5. Keep device operating systems up-to-date
6. Encrypt your devices
7. Mobile security policies should fit into overall security framework
8. Install apps from trusted sources; consider building an enterprise app store
9. Provide cloud-sharing alternatives
10. Encourage users to install anti-malware on their devices

Tips for a Malware-Free Smartphone

* Always research the publisher of the app.
* Read online reviews.
* Always check app permissions.
* Avoid directly installing Android Package files (APKs).
* Put a malware and antivirus scanner on your phone.
If security and privacy is more important than convenience, then disable:

- the Notification Center
- access to Siri and Passbook, and
- the Control Center.

Other measures to keep your information private include:

- Keep your web browsing private with Safari
- Revoke app access to your location
- Revote app access to your contacts
- Adjust privacy settings on Facebook
- Connect to a VPN
- Erase your browsing history and data
- Visit sites without making history
- Watch for suspicious websites

10 Common Mobile Security Problems to Attack

1. Mobile devices often do not have passwords enabled
2. Two-factor authentication is not always used when conducting sensitive transactions on mobile devices
3. Wireless transmissions are not always encrypted
4. Mobile devices may contain malware
5. Mobile devices often do not use security software
6. Operating systems may be out-of-date
7. Software on mobile devices may be out-of-date
8. Mobile devices often do not limit Internet connections
9. Mobile devices may have unauthorized modifications
10. Connecting to an unsecured Wi-Fi network could let an attacker access personal information from a device, putting users at risk for data and identity theft

Take Steps to Protect Your Mobile Phone

1. When choosing a mobile phone, consider its **security features**
2. Configure web accounts to use **secure connections**
3. **Do not follow links** sent in suspicious email or text messages
4. Limit exposure of your **mobile phone number**
5. Carefully consider what **information you want stored** on the device
6. **Be choosy** when selecting and installing apps
7. Maintain **physical control** of the device, especially in public or semi-public places
8. **Disable interfaces** that are not currently in use, such as Bluetooth, infrared, or Wi-Fi
9. Set Bluetooth-enabled devices to **non-discoverable**
10. **Avoid joining** unknown Wi-Fi networks and using public Wi-Fi hotspots
11. Delete all information stored in a device prior to **discarding it**
12. **Be careful** when using social networking applications
13. Do not “root” or “jailbreak” the device
How to Protect a Mobile Phone from Being Stolen

1. **Keep details:** Your phone number, make and model, color and appearance details, pin or security lock code, IMEI number
2. Add a security mark using an ultra violet pen to you handset and battery
3. Use the security lock code, or PIN feature, to lock your phone
4. Make a lime-green color gel for your phone’s display (i.e., make it look old)
5. Install anti-phone theft software
6. Never let the phone out of your sight

**If stolen:**
1. Have your phone number disabled
2. Request an immediate, formal investigation from your carrier
3. File a police report immediately

http://www.wikihow.com/Protect-a-Mobile-Phone-from-Being-Stolen
Protecting Your Tablet in Case it is Lost or Stolen

* Use a combination of **encryption and remote wiping**.
* Set a **passcode** on your iPad and your data will be automatically encrypted.
* Set ‘Require Passcode’ for no more than **15 minutes** and **turn Erase Data on**.
* Turn **data protection on** because it encrypts your e-mail messages and their attachments. It also affects Messages, Calendar, Contacts, Photos, and Health data values.
* Use the **Configuration Utility** to open up a suite of additional security settings.
* Set the Security drop-down to ‘Always’ so that you can remove the profile.
* **Enable remote wipe** to allow you to delete the data on a lost iPad if and when it connects to the Internet.
* Follow good safety practices by using **VPN**.
* If you loose your iPad, **change your password settings** on any services that you have connections for.

Report the loss to your organization and/or mobile service provider.

- If your phone or PDA was issued by an organization or is used to access private data, notify your organization of the loss immediately.
- If your personal phone or PDA was lost, contact your mobile phone service provider as soon as possible to deter malicious use of your device and minimize fraudulent charges.

Report the loss or theft to local authorities. Depending on the situation, it may be appropriate to notify relevant staff and/or local police.

Change account credentials. If you used your phone or PDA to access any remote resources, such as corporate networks or social networking sites, revoke all credentials that were stored on the lost device. This may involve contacting your IT department to revoke issued certificates or logging into websites to change your password.

If necessary, wipe the phone. Some mobile service providers offer remote wiping, which allows you or your provider to remotely delete all data on the phone.
How You Can Fight Back

1. Enable user authentication
2. Verify the authenticity of downloaded applications
3. Install antimalware capability
4. Install a firewall
5. Install security updates
6. Remotely disable lost or stolen devices
7. Enable encryption for data stored on device or memory card
8. Enable whitelisting
9. Establish a mobile device security policy
10. Provide mobile device security training
11. Establish a deployment plan
12. Perform risk assessments
13. Perform configuration control and management

NIST Special Publications
