My CEO wants an iPad...now what?

Mobile Security for the Enterprise
Agenda

• Introductions
• Emerging Mobile Trends
• Mobile Risk Landscape
• Response Framework
• Closing Thoughts
Introductions

Amandeep Lamba
Manager
IT Risk & Security Assurance
PwC

amandeep.lamba@us.pwc.com
(301) 943-8800
Emerging mobile trends
## Mobile Adoption in the Workplace

<table>
<thead>
<tr>
<th>Personally owned devices</th>
<th>Personally owned devices can contain applications, preferences, and configuration settings that could increase the risk to sensitive corporate information that resides on the devices. Additionally, the organization's decision to wipe data from a device is less clear-cut because there may be personal data on the device as well.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate-owned devices</td>
<td>Corporate-owned devices provide the freedom to manage and control the devices and information on them at the organization’s disposal. This enables more secure control of a device's behavior, but it can increase cost to the organization, and many users now expect more freedom in using their own device.</td>
</tr>
<tr>
<td>Mobile consumer applications</td>
<td>Businesses are creating mobile applications to increase consumer interaction and satisfaction. These applications must be vetted by the organization’s information security department. Mobile applications can increase an organization’s threat landscape by opening access to consumers’ sensitive information that is personally identifiable, financial, or medical.</td>
</tr>
<tr>
<td>Mobile corporate applications</td>
<td>Internally facing applications can increase productivity and employee satisfaction as well as foster innovation in the organization. However, to transform business processes, these applications normally need access to sensitive company information. Executives are now asking for access to real-time data including company financials. This access presents both a business opportunity and an information security risk that companies must address.</td>
</tr>
</tbody>
</table>
**Emerging Trends**

**Business Drivers**

1. Mobile Devices with Advanced Capabilities and Fast Network Connectivity

2. User Driven Change:
   - Board Room and Senior Executives driving usage
   - Users demanding enhanced collaboration and productivity

3. Greater convenience:
   - Applications moving beyond Email/Contacts/Calendars
   - Rich content enables quick decisioning

**Key Trends**

1. BYOD/Approved Corporate Mobile devices
2. Compelling Mobile Applications
3. Data-driven Approach to Mobile Security
4. Cloud Applications, Data and Services
5. Mobile Access to Social Networking
6. Mobile Governance and Monitoring
Emerging Trends

Percent of companies using apps to secure their data: 50%

Percent of companies using MDM to secure their data: 30%
Emerging Trends

Percent of Global 500 deploying or testing the iPad: 47%

Percent of Global 500 deploying or testing the iPhone: 57%
Mobile risk landscape
“Nearly 30% of companies experienced a breach due to unauthorized mobile device use.”

Source: Q1 Enterprise and SMB Survey, 2009 - Forrester Research
Lost or stolen devices - the number one threat associated with mobility programs

- 56% of us misplace our **cell phone** or laptop each month
- 113 **cell phones** are lost or stolen every minute in the U.S.
- 120,000 **cell phones** are lost annually in Chicago taxi cabs
- 25% of Americans lose or damage their **cell phone** each year
- Major city transit authorities receive over 200 lost items per day

Source: MicroTrax Study, 2011
Other threats to mobile devices

- Feb 2012 – Mobile social network Path caught uploading users’ address books to their network without approval
- Jan 2012 – Up to 5 million Android users download 13 malware infected applications from Google’s Android Market
- Jan 2012 – QR Codes used to trick users to visit mobile spam sites
- Dec 2011 – CarrierIQ tracking software found on a wide range of devices
- Oct 2011 – Device manufacturer HTC admits vulnerability in their phones that can cause unauthorized access to data
- Sept 2011 – German security firm G Data reports mobile malware increased 270% during the first six months of 2011 with 1.2 million new valiants
Current situation

Responses to PwC’s 2012 Global State of Information Security Survey underscore the need for institutions to improve mobile security due to the increased use of mobile devices to access data.

Fewer than half of the respondents have mobile and social media security strategies.

Q: “What process information security safeguards does your organization currently have in place?” (Not all factors shown; total does not add up to 100%).

Data security breaches have increased at a faster pace than any other security incident.

Q: “What types of security incidents (breach or downtime) occurred?” (Respondents were able to select more than one type of security. As a result, percentages do not add up to 100%).

---

**Typical mobile device risks**

**Smartphones and tablets at work:** Workers utilize corporate and personally owned devices to access corporate services such as email and calendar, time and expense, and collaboration systems via a private cloud.

**Mobile interactive marketing:** Marketing campaigns extend to mobile devices through QR codes that send consumers to a company’s mobile website, where they can download a mobile app and receive a coupon for a discounted product.

**Mobile customer care:** The desktop extends to the customer for activities such as portfolio/claims reviews at lower costs and an enhanced customer and worker experience. Customers can use their same devices to comment on the brand via their social network.

---

**Privacy**
1. Protecting corporate intellectual property and trade secrets on the mobile device
2. Protecting customer account information on the device, upon transmission and throughout the account life cycle
3. Protecting the privacy of customer transactions conducted via the mobile device at the behest of the customer

**Financial loss**
1. Preventing exploitation of intellectual property and trade secrets by adversaries
2. Preventing unauthorized transactions on customer accounts that result from compromises of a device or authorized user credentials
3. Protecting from fraudulent sales/enrollment that occurs from impersonation in the event of a lost or stolen device or credentials

**Compliance**
1. Anti-money laundering
2. Consumer breach notification
3. International data safety regulations
4. Privacy regulations
5. Financial loss/anti-fraud regulations
Complicating factors for mobile security

- Device Diversity/Complexity
- Application Explosion
- Data Explosion
- Advanced Persistent Threats
- Data Transference and Inference
Response framework
Establish Governance Model
Define corporate stance on mobile strategy

Define Policies & Procedures
Define and publish organizational policies which reflect governance strategy

Analyze Risk Posture
Perform risk analysis to ensure alignment between projected and actual risk levels

Deployment
Deploy mobile strategy in organization

Operations & Management
Sustainability and long term operations
# Mobile deployment

## Mobile security policy

## Mobile device standards

<table>
<thead>
<tr>
<th>User-to-device interaction</th>
<th>Device-to-device interaction</th>
<th>Device management</th>
<th>Device protection</th>
<th>Policy management</th>
<th>Mobile applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Authentication</td>
<td>• Authentication</td>
<td>• Provisioning /</td>
<td>• Enable/disable</td>
<td>• Access control</td>
<td>• Memory mgmt.</td>
</tr>
<tr>
<td>• Access / privilege</td>
<td>• Authorization</td>
<td>de-provisioning</td>
<td>• Policy</td>
<td>• Policy update</td>
<td>• Secure storage &amp;</td>
</tr>
<tr>
<td>• Encryption</td>
<td>• Encryption</td>
<td>• Asset tracking</td>
<td>enforcement</td>
<td>• Approved</td>
<td>encryption</td>
</tr>
<tr>
<td>• Training / awareness</td>
<td>• Encryption</td>
<td>• Patching /</td>
<td>• Anti-malware</td>
<td>software</td>
<td>• SDLC integration</td>
</tr>
<tr>
<td>• Policy acknowledgment</td>
<td>• Transaction integrity</td>
<td>updates</td>
<td>• Intrusion</td>
<td>• Standard config</td>
<td>• Application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Location</td>
<td>detection and</td>
<td>• Backup/Recovery</td>
<td>provisioning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device security</td>
<td>prevention</td>
<td>• Audit trails and</td>
<td>• Application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>support</td>
<td>• Forensics</td>
<td>incident mgmt.</td>
<td>security support</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cost mgmt.</td>
<td>• Device integrity</td>
<td>• Compliance</td>
<td>and testing</td>
</tr>
</tbody>
</table>

- • Access control
- • Policy update
- • Approved software
- • Standard config
- • Backup/Recovery
- • Audit trails and incident mgmt.
- • Compliance
# Mobile protection technologies

Before deploying mobile technology to their employees, institutions need to be confident that the corporate data is secure. Leading institutions are adopting a range of mobile protection technologies.

## Mobile Device Management (MDM)
- Secures, monitors, and manages enterprise mobile devices and can act as a proxy for device activity (such as web browsing and email), depending on the vendor solution.
- Device activity is filtered, based on management defined policies.
- Devices receive and execute management commands from a central server.
- Vendors: MobileIron, Sybase Afaria, AirWatch, RIM, McAfee.

## Secure Application Container
- Corporate data (email, contacts, internal web sites, etc.) is encrypted within a secure application that is firewalled from the rest of the operating system.
- Data transfer occurs between the mobile device and a secure application server via an encrypted channel.
- Vendors: Good for Enterprise, GoodReader, BoardVantage, SAP BusinessObjects.

## Device Virtualization
- Mobile devices use a hypervisor to create secure separation between underlying hardware and secure software that runs on top of it.
- Device virtualization enables multiple OSs or virtual machines to segregate personal and corporate information and use.
- Vendors: VMWare, Citrix.

## Antivirus
- Scanning capabilities depend on the nature of the OS and the server.
- Some antivirus tools are limited to scanning file attachments on the device and server, while others are capable of scanning applications, settings, data, and media files for malware.
- Vendors: Lookout (Android), Intego’s VirusBarrier (iOS), AVG (Android).
“Bring Your Own” Device security considerations

• Many organizations have now opted to allow employees to procure their own devices which will ultimately connect to enterprise data and resources

• A “Bring Your Own” strategy presents additional security and privacy challenges which should be carefully considered prior to implementation

• Policies must be carefully crafted that mandate certain restrictions on the employee’s access to corporate data with a personally owned device. Policies should cover minimum device security standards, use of anti-virus or endpoint security software based on legal or compliance requirements and clear language regarding consent for the enterprise to access enterprise data on the device on a timely basis.

• The enterprise should aggressively monitor access by employees with personally owned devices and consider restricting access to the minimum level required to perform the employee’s role (e.g. e-mail and calendar)

• The enterprise should reserve the right to rapidly bar access to data and resources by employees with personally owned devices if necessary to protect enterprise data, address newly identified risks or to comply with legal or compliance requirements

• It is becoming increasingly hard to operate a BYOD program without using a Mobile Device Management (MDM) platform
Common BYOD challenges and risks

• BYOD increasingly reopens traditional debates on use of personally owned laptops and computing equipment (i.e. Macs, external storage, printers)

• Use of personally owned devices blurs owner responsibilities regarding device support, ownership of data and how much access and control the organization may have to data on the device

• There is still frequent resistance by users to sign acknowledgements or acceptable use agreements (“It’s my device!”)

• Users want the latest smartphone, regardless of what operating system or features the organization is able to support

• Users have little incentive to report lost or stolen devices on a timely basis. In many cases the organization will only learn of a lost device when the user requests access for a new device
Closing thoughts
Enterprise Deployment

Review Impact to Enterprise Defense in Depth Strategy

Specifically consider the following areas:

- Authentication
- Segmentation
- Encryption
- Monitoring
Key considerations

1. How will you govern and manage personally owned devices, and which platforms should we support?
2. What kinds of corporate applications and resources should do you open to mobile devices?
3. How will you educate your customers, employers, and partners about mobile risks?
4. How can you balance mobile productivity, opportunity, and risks?
5. How do you increase consumer interaction and satisfaction through mobile devices while protecting the consumer and your brand?
6. How will you evolve processes and tools to accommodate mobile devices?
Amandeep Lamba
Manager
IT Risk & Security Assurance
PwC
amandeep.lamba@us.pwc.com
(301) 943-8800