# Agenda

<table>
<thead>
<tr>
<th>I</th>
<th>Introduction – Mobile Device Security: Expediential Growth in Mobility</th>
</tr>
</thead>
<tbody>
<tr>
<td>II</td>
<td>Business Drivers for Mobility</td>
</tr>
<tr>
<td>III</td>
<td>Mobile Security Considerations</td>
</tr>
<tr>
<td>IV</td>
<td>Risk Mitigation – An Approach to Mobile Security</td>
</tr>
<tr>
<td>V</td>
<td>Secure mobile software development - why is this paramount?</td>
</tr>
<tr>
<td>VI</td>
<td>Wrap-up / Q&amp;A</td>
</tr>
</tbody>
</table>
Mobile Device Security

I. Introduction - Expediential Growth in Mobility
Connected Mobile Devices – Expediential Growth

“It took 22 years to connect 2 Billion people to the internet – The next 2 billion will come online in 5 years”

Gary Kovacs (Mozilla)
The proliferation of mobile devices

3 billion tablets and smart phones globally by 2015 - the Economist “the World in 2013”
**Mobile device proliferation has changed the game**
Computing will shift increasingly to mobile devices.

<table>
<thead>
<tr>
<th>Worldwide Device Shipment (thousands)</th>
<th>2012</th>
<th>2013</th>
<th>2014 (Projected)</th>
<th>2017 (Projected)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Type</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC</td>
<td>341,263</td>
<td>315,263</td>
<td>302,315</td>
<td>271,612</td>
</tr>
<tr>
<td>Ultramobile</td>
<td>9,822</td>
<td>315,229</td>
<td>38,687</td>
<td>96,350</td>
</tr>
<tr>
<td>Tablet</td>
<td>116,113</td>
<td>197,202</td>
<td>265,731</td>
<td>467,951</td>
</tr>
<tr>
<td>Smart Phones</td>
<td>1,748,176</td>
<td>1,875,774</td>
<td>1,949,722</td>
<td>2,127,871</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>2,213,373</td>
<td>2,411,796</td>
<td>2,556,455</td>
<td>2,964,783</td>
</tr>
</tbody>
</table>

*Source: Gartner, April 2013*
Mobile is an essential channel to gain presence and strengthen consumer and employee engagement.

Mobile is reaching ubiquity very quickly...

...is becoming a differentiator...

...and is changing the way users are engaging with businesses...

15,000 Applications released weekly

Mobile phone adoption significantly outpaced recent technologies

- 94% Of Fortune 500 firms have deployed or are testing iPads for staff.
- 82% Smartphones represent only 12% of total global handsets, 82% of traffic.

Length in Years to Reach 50M Users

- Radio: 38 years
- Television: 13 years
- PC: 4 years
- iPod: 3.6 years
- iPhone: 2.5 years
- iPad: 1.5 years

- PC: 75K
- Droid: 675K
- iPad: 225K
- iPhone: 575K

Mobile is reaching ubiquity very quickly...

...is becoming a differentiator...

...and is changing the way users are engaging with businesses...

15,000 Applications released weekly

Mobile phone adoption significantly outpaced recent technologies

- 94% Of Fortune 500 firms have deployed or are testing iPads for staff.
- 82% Smartphones represent only 12% of total global handsets, 82% of traffic.

Length in Years to Reach 50M Users

- Radio: 38 years
- Television: 13 years
- PC: 4 years
- iPod: 3.6 years
- iPhone: 2.5 years
- iPad: 1.5 years

- PC: 75K
- Droid: 675K
- iPad: 225K
- iPhone: 575K
# Mobility challenges, then vs. now

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope of the mobile challenge</strong></td>
<td>Limited to several types of company issued devices.</td>
<td>User’s demand freedom of choice. Hundreds of devices.</td>
</tr>
<tr>
<td><strong>Ownership &amp; accountability</strong></td>
<td>IT led and operated.</td>
<td>IT operated, IT or user owned.</td>
</tr>
<tr>
<td><strong>Applications &amp; content</strong></td>
<td>Primarily email and contacts.</td>
<td>Rich content and applications, mobile VPN, a desktop like experience.</td>
</tr>
<tr>
<td><strong>Connectivity</strong></td>
<td>Primarily enterprise data center.</td>
<td>Enterprise, cloud and hybrid scenarios.</td>
</tr>
<tr>
<td><strong>Cultural adoption</strong></td>
<td>Primarily a work device.</td>
<td>Personal entertainment device, social hub, blending of work/life. (Consumerization of IT)</td>
</tr>
</tbody>
</table>
Mobile Device Security

II. Business Drivers for Mobility
### Business Drivers

**User driven change**
- Board Room and Senior Executives driving usage
- Users demanding enhanced collaboration and productivity
- Increased consumerization fostering a culture of instant gratification

**Greater convenience**
- Applications moving beyond Email/Contacts/Calendars
- Mobile capabilities and applications aligning with the business model
- Rich content enables quick decisions

### Impact & Trends

- Infrastructure to support increased adoption of Smartphones
- BYOD/approved corporate mobile devices
- Security, compliance, and legal consideration
- Mobile/cloud applications, data and services
- Need for stronger mobile governance and monitoring
Why is mobile security complex?

- Device Diversity/Complexity
- Application Explosion
- Data Explosion
- Advanced Persistent Threats
- Data Transference and Inference
Primary Mobile Attack Vectors

Data Transference and Inference

Physical loss or theft of the device

Malicious software
BYOD Challenges

#1 Protecting business information and intellectual property is the number one challenge for organizations implementing BYOD

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’s my device!”

There is still frequent resistance by users to sign acknowledgements or acceptable use agreements

Diversity of mobile platforms: Users want the latest, regardless of what operating system or features the organization is able to support
Mobile Device Security

III. Mobile Security Considerations
Why is mobile security a concern?

Mobile threats are on the rise according to the Symantec Report of 2012;

31 percent of all mobile users have received an SMS from someone that they didn't know. An example is where the user receives an SMS message that includes a link or phone number.
**Mobile Phishing**

1. You receive an e-mail from your bank.
2. The end-user will select the link: `http://www.yourbankname.example.com`.
3. The URL link will actually point to: `http://badbackersite.example.com`.

The best method around this is:

A. Never press a link directly in a mail message.
B. If you are not sure - contact your bank and ask if they are sending messages with Links. Most banks today are not sending messages with URL in s.
C. If you still think this is a real message - don’t select the link inside the message. Copy the link and paste the link into a browser.
D. Finally - most to all banks will use encryption. This is the HTTPS that you will see as part of a URL. If you get any 'strange' prompts when you use HTTPS - then contact your bank and ask them if they sent you this message.
## Mobile Security Key Considerations

<table>
<thead>
<tr>
<th>Threat Modeling</th>
<th>• Does your organization continually review and assess new threats against its mobile device strategy by assessing relevant security related documentation and configurations?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controls &amp; Technical Assessments</td>
<td>• How often are controls and the MDM solutions evaluated to identify control deficiencies, security risks and known vulnerabilities?</td>
</tr>
<tr>
<td>Controls &amp; Technical Remediation</td>
<td>• Are deficiencies and security gaps acted upon? Are additional controls implemented or existing controls strengthen?</td>
</tr>
</tbody>
</table>
## Other Mobile Security Considerations

1. How should we govern and manage personally owned devices, and which platforms should we support?

2. What kinds of corporate applications and resources should we open to mobile devices?

3. How will we educate our customers, employers, and partners about mobile risks?

4. How can we balance mobile productivity, opportunity, and risks?

5. How do we increase consumer interaction and satisfaction through mobile devices while protecting the consumer and our brand?

6. How will we evolve processes and tools to accommodate mobile devices?
Global State of Information Security Survey Results - A worldwide study

The Global State of Information Security® Survey 2014, a worldwide study by PwC, CIO Magazine, and CSO Magazine, was conducted online from February 1, 2013 to April 15, 2013.

- PwC’s 15th year conducting the online survey, 10th with CIO and CSO magazines
- Readers of CIO and CSO magazines and clients of PwC from 128 countries
- More than 9,300 responses from CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security
- More than 40 questions on topics related to privacy and information security safeguards and their alignment with the business
- Thirty-three percent (33%) of respondents from companies with revenue of $500 million+
- Margin of error less than 1%
Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace with use

Smart phones, tablets, and the “bring your own device” trend have elevated security risks. Yet efforts to implement mobile security programs do not show significant gains over last year, and continue to trail the proliferating use of mobile devices.

Initiatives launched to address mobile security risks

- Mobile security strategy: 40%, 42%
- Mobile device-management software: 38%, 39%
- Protect corporate e-mail and calendaring on employee- and user-owned devices: 36%, 37%
- Strong authentication on devices: 31%, 35%
- Ban of user-owned devices in the workplace/network access: 33%, 30%
- Use of geolocation controls: N/A, 19%

Source: PwC Global Survey of Information Security 2014

Question 16: “What initiatives has your organization launched to address mobile security risks?” (Not all factors shown.)
Security incidents are increasing, with awareness of mobile security issues a key issue

The number of incidents detected in the past 12 months increased by 25%, perhaps an indication of today’s elevated threat environment. Respondents who do not know the number of incidents doubled over two years. This may be due to continued investments in security products based on outdated models.

Mobile device (e.g., smart phone, tablet computer) exploited:
All respondents, 21%

* A security incident is defined as any adverse incident that threatens some aspect of computer security.

Question 18: “What is the number of security incidents detected in the past 12 months?”
Mobile Security

IV. Risk Mitigation – An Approach to Mobile Security
Achieving Mobile Security

Develop a Strategy
- Develop a business case
- Develop use cases and patterns
- Define implementation roadmap and setup a PMO

Show Quick Wins
- Create policies, standards, and procedures
- Secure the mobile environment
- Develop stop gap measures to promote consistent deployment

Build a Governance Model
- Develop a model that includes roles, responsibilities, and decision flow charts for managing the direction of the program

Analyze and Address Risk
- Perform risk assessment
- Migrate to consistent MDM platform
- Identify BYOD implications

Deploy Mobile Strategy
- Implement key processes, technologies, controls, and user awareness initiatives

Operate and Maintain
- Measure and report on key program metrics
- Monitor compliance

Achieving Mobile Security Maturity
Mobile Security Deployment

Mobile security policy

Mobile device standards

User-to-device interaction
Device management
Device protection
Policy management
# 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). |
Mobile Security

V. Secure mobile software development - why is this paramount?
Secure software development

Organizations that *embroider security* into their mobile software development processes have less internal and external exposure to compromise.
Secure software development – The Models

BSIMM – Building Security in Maturity Model

Microsoft SDL (Secure Development Lifecycle)

Software Assurance Maturity Model

NIST 800-64

ISO/IEC 27034-1
**BSIMM – Building Security in Maturity Model**

**Overview**
- BSIMM built BSIMM by gathering real data from nine large-scale software security initiatives (i.e. Adobe, EMC, Google, Microsoft, QUALCOMM)—only activities observed in the field could be added to the model
- Framework composed of four domains and over 100 secure SDLC activities

**Lessons Learned**
- “Auditable” and defendable framework composed of prescriptive and measurable activities
- Flexible framework which is used as general guidance—i.e. as a trail guide rather than as a cookbook
- While there are prescriptive domains and objectives the associated activities used to meet the requirements can be customized for the client’s environment
- SDLC process agnostic
- Model has been validated with data from 67 firms
- Adopted by major firms such as Google and Sony
- Can also be used as a yardstick for measuring existing practices against industry peers
## Microsoft SDL

### Overview
- Originally built internally as Microsoft-wide initiative and a mandatory policy since 2004
- Later extended and made public for wider adoption
- Collection of mandatory security activities, presented in the order they should occur and grouped by the phases of the traditional software development life cycle
- MS-only versions since public release

### Lessons Learned
- Can be applied directly to Spiral and Waterfall development models
- Threat Modeling is the ‘cornerstone’ of SDL
- Microsoft has openly stated that all current mandatory application security related policies, standards, and procedures along with their supporting people, processes, and tools “meet or exceed” the guidance in ISO/IEC 27034-1 as published in 2011
- Heavyweight model which has proven difficult for certain shops to adopt - good for experts to use as a guide, but hard for non-security folks to use off the shelf
## NIST SP 800-64

### Overview
- Guideline developed to assist federal government agencies in integrating security steps into SDLC
- Guideline applies to all federal IT systems other than national security systems
- Guide includes general five phased SDLC and each phase includes a minimum set of security steps needed to effectively incorporate security into a system during its development.

### Lessons Learned
- NIST publications often viewed as “gold standard” for security, however, there is little evidence of adoption in the private sector
- Often viewed as overly complex and unwieldy
- The NIST model is a process model more related to the SDL/CLASP/TouchPoint type of models
- NIST model is waterfall-based
- Focuses much more on deployment, operations and disposal than the other models
**ISO/IEC 27034-1**

**Overview**

- Officially released in 2011 and provides an overview of application security concepts as well as the framework and processes that are needed to operate a comprehensive application security program
- Part one of six-part standard, remaining five parts will provide additional depth, but are not yet published
- Developed by the same group that developed ISO/IEC 27001 series

**Lessons Learned**

- Relatively new entrant to the secure software framework discussion – little to no insights into reception by marketplace
- Standard specifically avoids recommending specific security controls within a development lifecycle, and it does not prescribe any specific technology
- Not dependent upon ISO/IEC 27001 and can be used independently, however it is viewed as a complement to ISO/IEC 27001
- “Auditable” and defendable framework
- Given track record of ISO 27000 series many view this framework as being accessible to enterprises, IT auditors, regulatory bodies, software producers, and others to incorporate as necessary into their existing initiatives
Comparing Microsoft SDL to BSIMM

The following criteria was utilized for comparing the strengths and limitations of the Microsoft SDL and BSIMM frameworks.

<table>
<thead>
<tr>
<th>Implementation</th>
<th>The delivery of the program must be flexible to allow for an organization to adopt and instill the framework into its unique environment without significant disruption to its existing practices and with available budget and resource.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution</td>
<td>The execution of the program will meet the objectives of the organization’s governance obligations in addition to delivering an effective framework for assuring the security posture of software.</td>
</tr>
<tr>
<td>Sustainability</td>
<td>The quality and evolution of the secure software program must be maintained. As the organization changes direction, the framework must be adaptable to fit future business strategy.</td>
</tr>
</tbody>
</table>
## Comparison Results

<table>
<thead>
<tr>
<th>Criteria</th>
<th>BSIMM</th>
<th>Microsoft SDL</th>
</tr>
</thead>
</table>
| **Implementation** | • Holistic approach to a software security program by incorporating corporate governance and metrics to evaluate controls.  
• BSIMM can be used to plan, structure, and execute the evolution of an organization’s software security initiative. | • Provides a sequential roadmap for secure software development implementation.  
• Complicated framework to incorporate due to the level of obscurity and complexity.  
• Absence of tangible control activities that can be audited on a recurring basis. |
| **Execution** | • The execution of the BSIMM will illustrate pursuit of internal software compliance by requiring governance within the program.  
• The BSIMM encompasses planning and assigning roles and responsibilities, identifying software security goals, determining budgets, and identifying metrics and gates. | • Microsoft offers tools and templates to assist with the execution of the framework.  
• The execution of the MS SDL is a very rigid approach.  
• Lacks incorporation of organizational goals and compliance obligations.  
• Does not include guidance for law, policy, and procedure compliance into the software program. |
| **Sustainability** | • Key performance indicators enable continuous performance and benchmarking progress against previous points in time.  
• Metrics can be leveraged to analyze results in contrast to other peers in industry. | • Eliminates redundancies and coordinate processes, thereby streamlining the efficiency of future application development.  
• Absence of scalability and limited ability to tie the program with the goals and desires of the business.  
• Lacks ability to measure and gauge performance over course of time. |
Comparison of secure software frameworks – MS SDL versus BSIMM (slide 1 of 3)

The following is a detailed comparison of two secure software frameworks: MS SDL and BSIMM. The comparison on this slide includes a summary of pros and cons of each framework based on the following attributes: Acceptability as an audit framework and ongoing maturity assessment.

<table>
<thead>
<tr>
<th>Key Component Areas</th>
<th>BSIMM</th>
<th>MS SDL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acceptability as an audit framework</strong></td>
<td>BSIMM is a vendor agnostic framework that was designed by experts from Independent Software Vendors (ISVs), high tech, and financial services industries. 67 major organizations have validated the BSIMM’s practicality for utilization. All of the activities produce artifacts sufficient to allow auditing for compliance adherence. There are 112 auditable control activities within the BSIMM Framework.</td>
<td>MS SDL was created and designed by Microsoft, and designed for small to medium sized organizations. Although MS SDL is recognized as a strong secure software development program, there is an absence of tangible control activities that can be audited on a recurring basis.</td>
</tr>
<tr>
<td><strong>Maturity Assessment</strong></td>
<td>BSIMM is a model that allows an organization to assess the current state of the software security program and subsequently measure the improvement of the program over time. Each practice within the framework is supplemented with 3 maturity levels.</td>
<td>MS SDL provides a one way road map that lacks in realm of regression to measure current performance metrics to gauge on how the software security program is performing over the course of time.</td>
</tr>
</tbody>
</table>
Comparison of secure software frameworks – MS SDL versus BSIMM – cont’ (slide 2 of 3)

The comparison continues by reviewing the practicality and feasibility of the two software frameworks.

<table>
<thead>
<tr>
<th>Key Component Areas</th>
<th>BSIMM</th>
<th>MS SDL</th>
</tr>
</thead>
</table>
| **Practicality**    | The BSIMM is an effective framework based on the thoroughness of the intelligence activities. BSIMM provides direction on how to establish organization-wide resources:  
  • Attack models to capture the attacker’s modus operandi.  
  • Security features and design to create usable patterns for major security controls.  
  • Standards and requirements practice to elicit explicit security requirements from the organization. | At it’s core, MS SDL is practical for a small archetype of organizations. However is not practical for organizations with strict governance programs as it does not include guidance for law, policy, and procedure compliance into the software program. |
| **Feasibility**      | BSIMM is sustainable, repeatable, and scalable. Sustainable due to ability to continuously measure performance with key performance indicators allowing comparisons against previous periods of time. Additionally, these metrics can be leveraged to analyze results in contrast to other peers in industry. BSIMM is scalable due to the ability to re-visit the program at periodic intervals to assess the as-is versus desired maturity state. | The MS SDL framework was designed for advanced software architects and engineers, it is a complicated framework to incorporate due to the level of obscenity and complexity. There is an absence of scalability as there is not a campaign to tie the program with the goals and desires of the business. |
**Comparison of secure software frameworks – MS SDL versus BSIMM – cont’**

The comparison continues by reviewing the flexibility of the two software frameworks.

<table>
<thead>
<tr>
<th>Key Component Areas</th>
<th>BSIMM</th>
<th>MS SDL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexibility</td>
<td>The core BSIMM framework is very versatile as it allows for the business to tailor fit the program based on the organization’s structure, size, and most importantly regulatory compliance obligations. The governance domain incorporates key control activities such as compliance and policy that offers specific guidance for stakeholders on strategies for auditability.</td>
<td>The Microsoft framework is rigid in nature as it doesn’t take into consideration the current state of the organization’s software security program. The MS SDL five phases are, Requirements, Design, Implementation, Verification, and Release. None of these phases incorporate an architectural analysis that constructs a risk assessment and remediation plan.</td>
</tr>
</tbody>
</table>
# Summary of Comparison of secure software frameworks – MS SDL versus BSIMM

The following illustrates a summary strengths and weakness of each framework

<table>
<thead>
<tr>
<th>BSIMM</th>
<th>MS SDL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strengths</strong></td>
<td><strong>Weaknesses</strong></td>
</tr>
<tr>
<td>Holistic approach to a software security program by incorporating corporate governance and metrics to evaluate controls.</td>
<td>Framework not specifically designed for any industry sector.</td>
</tr>
<tr>
<td><strong>Versatile</strong> – can be leveraged by any organization as it is vendor agnostic, regardless of industry or scope.</td>
<td><strong>Time and effort</strong> – If implemented prescriptively and at the highest level of maturity, a significant amount of time is required to build the program.</td>
</tr>
<tr>
<td>Control activity driven which makes it very auditable in a precise fashion.</td>
<td>Tools are available to test software security.</td>
</tr>
</tbody>
</table>
Visibility of mobile configuration—Configuration Management Database (CMDB)

What is a CMDB?

• A central database that provides **visibility and management** of application environments by establishing an inventory of configuration items (CIs).

• Maintains of **inventory** of application configuration parameters, including those parameters house or handle sensitive information.

• Included in **change management** workflow – provides additional layers of controls and monitoring for changes performed to environments that process sensitive information.

• Assists in the management of **complex environments** with interconnected heterogeneous systems.
Key takeaways...

Integrate security into the Enterprise Mobile Security Program.

Cultivate transparency of mobile security risks by asking key questions:

- What are the current risks within the mobile environment?
- What controls are in place today to address mobile security risks?
- What is the overall risk tolerance of management?
- Are all risks identified?
- Does ambiguity exist within mobile security processes and procedures?

Plan to incorporate mobile security safeguards into the infancy stages through completion of all future mobile enterprise projects.
References


Mobile Device Security

VI. Wrap-up / Q&A Session
Thank you...

For more information, please contact:

TR Kane
IT Risk & Security Assurance Partner
(216) 875-3038
t.kane@us.pwc.com

David Faraone
IT Risk & Security Assurance Manager
(412) 355-8023
david.a.faraone@us.pwc.com