



## Mobile Devices Security

API Conference  
Houston, November 12 2009  
Fabio Ottolini  
Security Services Manager - Schlumberger

Schlumberger

## Agenda

- i. Overview
- ii. Challenges
- iii. High Level Recommendations
- iv. Operational Recommendations
- v. Conclusions



Excellence in Execution

Schlumberger

## i. Overview

- Are they still mobile **phones**?



Motorola DynaTAC - 1983



iPhone 3GS - 2009

Excellence in Execution

Schlumberger

## i. Overview (2)

- Common features on mobile phones
  - Increased storage capacity, expandable via external media
  - Multiple connectivity options: Bluetooth, Wi-Fi, 3G, USB
  - Audio, video, and photos recording/playback
  - App install
  - GPS
- Comming next
  - Bluetooth 3.0, Wi-Fi Direct, Gobi, LTE...



Mobile Phones = Mobile Computers

Excellence in Execution

Schlumberger

## ii. Challenges

- Differences based on region/country/mobile carrier:
  - Device models
  - Features
  - Network features and coverage
  - Data/voice plans
  - Roaming agreements
  - OEM operating systems
  - Subsidies

**Pricing may be the most important factor in the decision process on the local level if a clear strategy is not defined on the global level**



Excellence in Execution

Schlumberger

## ii. Challenges (2)

- User awareness
  - Costs
  - User expectations
  - Security policies/best practices
  - Documentation: Quick guides and HOW TOs
- Change Management
  - Testing
  - What is going to be affected?



**How to manage an environment full of "unknowns"?**

Excellence in Execution

Schlumberger

### iii. High Level Recommendations

- Standardize as much as possible, respecting local limitations
  - Standardization on the operating system level is recommended
  - Standard image and devices, why not?
  - Supporting all operating systems is impractical, but...
  - Concierge VIP support is a must have
- Develop local competencies
  - On the Global Service Desk level, do not expect all analysts to be SMEs
  - Provide remote support when possible
- Involve Procurement all the way down to the local level
- Make sure users understand the main drivers behind policies/standards
- Set the expectations accordingly

Excellence in Execution

Schlumberger

### iv. Operational recommendations

- Have a long term strategy for mobility, but be prepared to adjust
- **Device management platform is essential for security!**
  - One more reason to standardize
  - Deploy configuration files
  - Apply security patches and policies
  - Control installed apps and what can be done with the phone
  - Application integration
  - Native or Third-Party approach?
- Data encryption
- Enforce PIN/Auto-lock timeout

Excellence in Execution

Schlumberger

### iv. Operational recommendations (2)

- Define process to report lost/stolen device
  - Remote wiping and auto-destruct procedures
- Data backup/restore procedures
- Extensive use of certificates
- Costs associated with mobile phones are a huge security risk
  - Mobile carriers pretend to care
  - User awareness is essential
  - Be creative (Skype, for example)

Excellence in Execution

Schlumberger

### v. Conclusions

- **Secure!** Mobile devices can easily become the path of least resistance in terms of security as they get deeper and deeper in the organizations
- **Manage!** Do not let the mobile initiatives be entirely driven by the market or end users. Only the IT organization is able to understand all the implications related to embracing a certain platform/technology
- **Do!** No matter what is the business case, the demand for mobile services is out there. If IT does not provide the solutions, they will come from the business
- And always remember:

**Mobile Phones = Mobile Computers**

Excellence in Execution

Schlumberger

Thank you!!!

Excellence in Execution

Schlumberger