GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Mobile Phone Security
Key Challenges for 2010 and Beyond

Alan Goode
Managing Director, Goode Intelligence

Presentation Summary:

- **Goode Intelligence About Us – Who we are and what we do?**
- **Goode Intelligence mSecurity 2010 analyst report series**
- **Results from the GI 2009 mSecurity Survey Report**
- **Mobile Phone Security Threats and Risks:**
  - *What are the current and near-term information security threats/risks from using a mobile phone?*
    - *Virus/Malware*
    - *Data Loss*
    - *Voice eavesdropping – is GSM secure?*
    - *Prosumer use – blurring of lines between business and personal and impact on mobile phone security*
    - *Mobile Appstores*
- **Mobile Phone Security – Recommendations:**
  - *Practical steps for minimising the risk of mobile phones within business*
  - *Summary of mobile phone security products and services*

Goode Intelligence: About Us

- **Goode Intelligence (GI)** is a specialist provider of Information Security and Mobile Commerce research and analysis.
- Founded in 2007 by Alan Goode and headquartered in London
- GI provides two core research and analysis products:
  - **Off-the-shelf research reports** that are published regularly including;
    - ***Analyst research reports:*** market analysis, sizing and forecasting
    - ***Insight research reports:*** insight into emerging technologies and the business drivers for their adoption
  - **Bespoke research and analysis** including;
    - ***Custom analyst research reports***
    - ***Market Surveys***
    - ***Technical and marketing white papers***
- Prior to setting up GI, Alan spent over 20 years in the mobile commerce and information security industry where he held senior management positions for leading organisations including T-Mobile UK, De La Rue, Citibank and Atos Origin*.*

Goode Intelligence: Mobile Phone Security Series 2010

- Main direction for GI throughout 2010 is mobile phone security
- Includes publication of ***mSecurity 2010 Report Series*** and the ***GI mSecurity 2009 Survey Report.***
- The ***mSecurity 2010 Report Series*** is a comprehensive analysis of the market for mobile phone security products and services and will be published in three separate inter-locking reports:
  - ***The Mobile Phone as an Authentication Device 2010-2014 (published November 2009)***
  - ***Mobile Phone Anti-Virus Products and Services 2010-2014 (to be published in April 2010)***
  - ***Mobile Phone Protection Products and Services (voice and data encryption, anti-theft and backup) 2010-2014***
- ***mSecurity 2009 Survey Report*** published in three parts to coincide with the publication of the three analyst reports and investigates the current status of mobile phone security within business – results fed into analyst reports – ***"we needed quantitative data"***

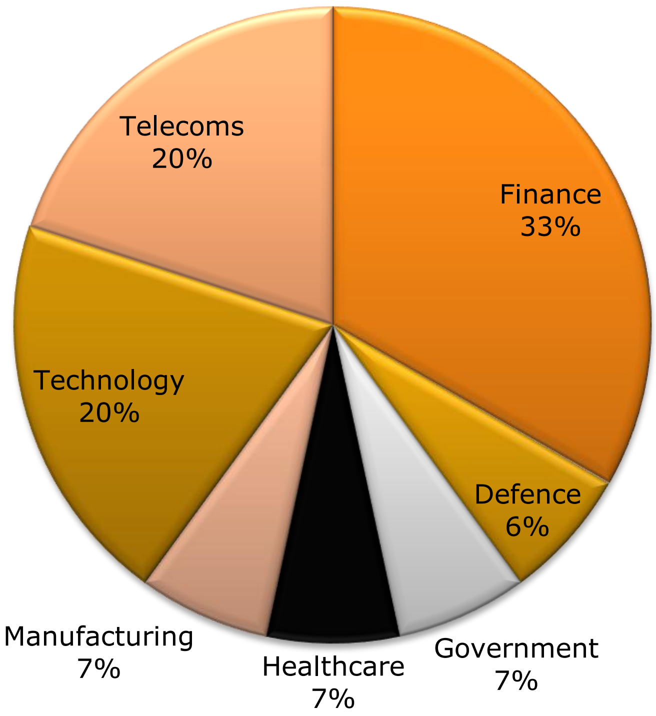
GI 2009 mSecurity Survey Report - Purpose & Participants:

- Most comprehensive vendor-independent survey on mobile phone security to date and published in three parts:
    - Part One: Access Control and Authentication
    - Part Two: Virus and Malware
    - Part Three: Protection Services, data (DLP) and voice encryption, anti-theft, firewall and backup

- Determines the current state of mobile security within businesses across the globe

- Specific emphasis on examining how smartphones like the iPhone and Google Android phone are altering the way that security professionals deal with enterprise security

Breakdown of respondents



GI 2009 mSecurity Survey Report: Policy and Regulation

- ***Mobile Policy:*** While 96% of organisations do have a documented security policy, some **46%** do not have a **specific documented security policy for mobile phones**

- **Acceptable Use Policy: 40%** do not cover mobile in their AUP

- **Standards: 45%** said that mobile was ***"covered slightly or not at all"***

- ***User Awareness:*** Of the 54% that do have a specific documented security policy that covers mobile phones, **50%** stated that they were either ***'not aware'*** or ***'did not know'*** whether users were aware

- ***Regulation:* 67%** of respondents are governed by industry or government regulation. **70%** state that these regulations did not cover mobile

- **Professional Awareness: 90%** of respondents felt that the current levels of awareness for mSecurity is not adequate

GI 2009 mSecurity Survey Report:
Procurement, Management and Deployment

- ***Procurement:*** Office Procurement responsible for **62%** of all mobile phone purchases and **40%** of information security departments have input into procurement

- **Management and Support: 47%** of organisations use an IT function to manage and support mobile phones.

Company use of personal mobile phones: 65% stated that they allowed employee-owned mobile phones to be used for business use (where business use includes voice calls, mobile email and mobile enterprise applications).

- ***Deployment:*** 80% feel that mSecurity is ***'very important'*** or ***'important'*** in the deployment of mobile phone based applications – ***"The sensitivity of general information in the company means that unencrypted mobile links are a very limiting factor."***

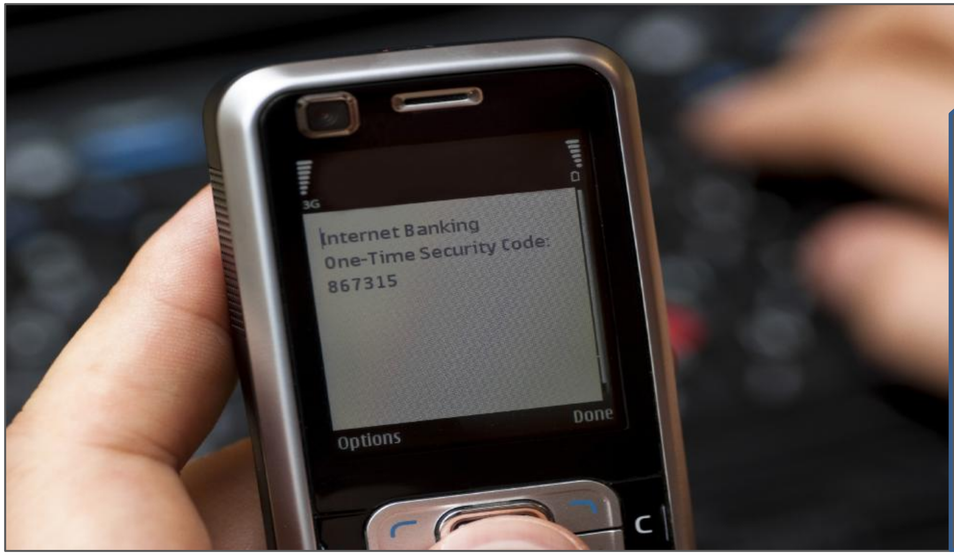
GI 2009 mSecurity Survey Report: Network Access

- ***Definition:*** The use of a mobile phone to access an enterprise network infrastructure (employee, consultant and trading partner etc.). Network could be local or remote.

- **Local Network Access:** A mobile phone using WiFi at work;
  - **30%** of organisations currently support mobile phones on their local data networks
  - A further **12%** planning to deploy within the next 12 months
  - Of the **58%** not supporting mobile phones, **40%** of these cited policy as an inhibitor to allowing network access

- **Remote Network Access:** Either using WiFi access point or at home/office or the mobile 3G network;
  - **42%** allow remote network access using a mobile phone
  - Of the **58%** not allowing remote access **33%** cited ***policy and regulation*** as a deterrent, **56%** stated ***'no business reason'*** and **11%** cited ***"didn't have the technology"*** to allow.

GI 2009 mSecurity Survey Report:
The Mobile Phone as an Authenticator



40 percent of organisations plan to deploy services and solutions that will enable employees to use their mobile phone as an authentication device by the end of 2011.

Technology Options:

- Server generated One Time Password (OTP) sent to mobile phone via SMS
- Soft token installed on a mobile phone that generates the OTP
- Voice authentication (user will receive an automated challenge via a voice call which they accept by entering the # key or a PIN)
- Mobile PKI

GI 2009 mSecurity Survey Report: Mobile Virus

- ***Anti-Virus Product Adoption:***
  - *Currently only **13%** of organisations have **deployed anti-virus** products on the phone*
  - ***54% plan to deploy within 12 months***
  - ***Why No? 37%** feel that **'there is no threat'**, **25%** feel that it is '**outside of remit'**, **25%** are **"not sure"** whether they have deployed*

- **Evidence: Will 2010 be the "year of the mobile virus"?**
  - ***Current Threat**: **87%** have **no evidence** of viruses on their employees mobile phones , **7% have seen viruses** and remaining **7% "do not know".***

- **Perceived Threat: Current perception is of low risk but rising**
  - **2009: 71%** state that there is a **'low'** risk of a mobile phone being infected with a virus with **21%** recording a **'medium'** risk.
  - **The Future Threat until 2011**: **21%** feel that the risk will be **'low'** with **50%** stating that the risk will be **'medium'**. Combined **28%** feel that the threat will increase and classify it as either **'high'** or **'very high'**.

GI 2009 mSecurity Survey Report: Data/Voice Encryption

- ***Data Encryption Product Adoption:***
  - *Currently 3**3%** of organisations have **deployed data encryption** products on the phone*
  - ***40% plan to deploy within 12 months***
  - *Remaining **27%** stated **‘no’***
  - ***Why No?: 45%** feel that **‘there is no threat’**, **11%** feel that it is ‘**outside of remit’**, **11%** are **‘not sure’** whether they have deployed, another **11%** feel that **‘there are no available products’**, a further **11%** state that it is **‘too difficult’** and the remaining **11%** state ‘**other reasons’***

- **Voice Encryption Product Adoption:**
  - *Currently **13%** have adopted third-party **voice encryption products***
  - ***14% plan to deploy within 12 months***
  - *Remaining **73%** stated **‘no’***
  - ***Why No?: 50%** feel that **‘there is no threat’**, **17%** feel that it is ‘**Too difficult to deploy’, 17%** are **‘not sure’** whether they have deployed, another **8%** feel that **‘it is outside of their remit’**, and the remaining **8%** state ‘**other reasons’***

GI 2009 mSecurity Survey Report: Backup and Data Wiping

- **Mobile Backup Adoption:**
  - *Currently **27%** of organisations have **deployed backup** products or services to protect data on phones*
  - ***73% have no products or no intention to deploy them***
  - ***Why No?: 37%** feel that **'there is no threat'**, **25%** feel that it is '**outside of remit'**, **64%** feel that '*__data on employee mobile phones does not require backup', 9%__ *are **"not sure"** whether they have deployed, a further **9%** say that it is **'too difficult to deploy'** and the remaining **18%** cited **'other'** reasons*

- **Mobile Data Wiping:**
  - *Currently **47%** have adopted **data wiping** products and services*
  - ***13%** are **'not sure'***
  - *•**40%** stated **'no'***
  - ***Why No?: 50%** feel that '*__data on employee mobile phones does not require wiping'__*, **33%** are **'not sure'** whether they have deployed and the remaining **17%** feel that **'it is outside of their remit'***

Mobile Phone Security Threats and Risks- Virus/Malware:

- **Evidence:**
  - **Small volumes**: Total of hundreds of variants as opposed to hundreds of thousands of viruses for desktop world that occur daily
  - **iPhone:** 2009 saw the emergence of viruses targeting ‘jailbroken’ iPhones – Hackers/Criminals are turning their attention to iPhone
  - **AV Vendors still waiting for *“the spike”***

- **Expert View:**
  - *"**20-30% of all mobile messaging traffic that is currently passing through the mobile operator network is either spam or malware” -*** mobile Anti-Virus vendor
  - A senior manager from one of the World’s largest security technology companies believes that *"**the threat [from mobile viruses] has not yet materialised",*** however the problem is ***"rubbing elbows“*** and that ***"the spike is very likely to occur very soon.”***

- **GI View: *The threat from mobile viruses is currently low but with the rising adoption of data-centric applications on Smartphones, including financial services, GI feels that the threat will rise from 2010 onwards***

Mobile Phone Security Threats and Risks- Data Loss:

- **Evidence:**
  - Storage of confidential data on phones is rising
  - Theft/Loss of mobile phones is substantial threat
  - Targeted attacks on key personnel
  - Impact of draft Data Protection law

- **Expert View:**
  - ***"There is an absolute need to encrypt the data on mobile devices when used in the enterprise"*** – Graham Cluley, SOPHOS

- **GI View:** ***Data Loss from mobile phones is the biggest current risk for users storing sensitive data on their mobile phones.***

Theft of Mobile Phone is Big Threat

Source: Credant

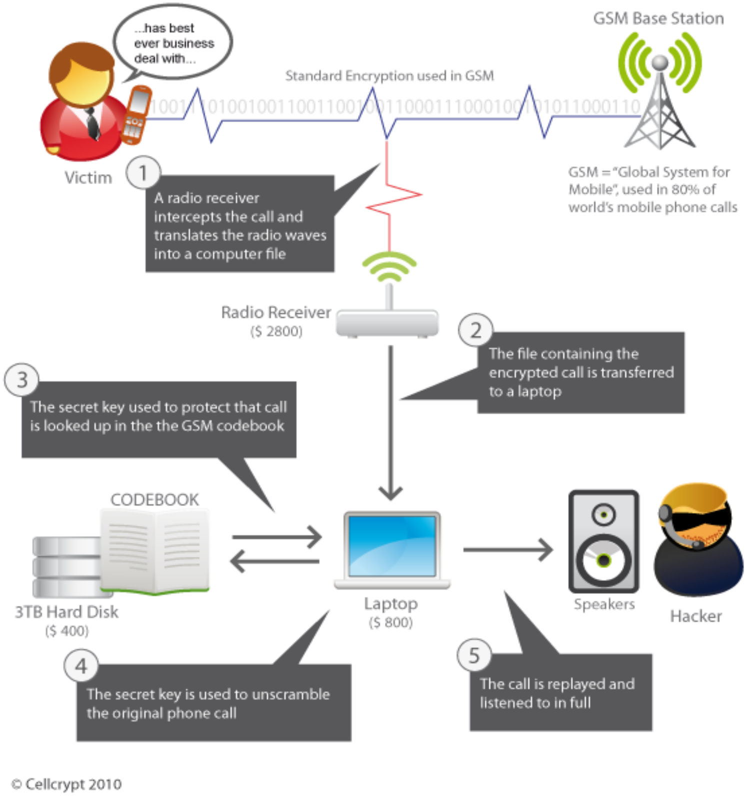
Mobile Phone Security Threats and Risks- Voice Threats:

- **Evidence:**
  - Reports that GSM encryption has been cracked
  - Cost of cracking codes has reduced in recent years
  - Not just GSM – 3G and CDMA also targeted
  - Known problems in using VoIP on mobile devices

- **Expert View:**
  - ***"It lowers the bar for people and organisations to crack GSM calls"*** – Ian Meakin, Cellcrypt

- **GI View: Confidential mobile voice calls should be protected with additional measures**

GSM Cracking Overview


...has best ever business deal with...
GSM Base Station
Standard Encryption used in GSM
Victim
GSM = "Global System for Mobile", used in 80% of world's mobile phone calls
Radio Receiver ($ 2800)
CODEBOOK
3TB Hard Disk ($ 400)
Laptop ($ 800)
Speakers
Hacker

1 A radio receiver intercepts the call and translates the radio waves into a computer file

2 The file containing the encrypted call is transferred to a laptop

3 The secret key used to protect that call is looked up in the the GSM codebook

4 The secret key is used to unscramble the original phone call

5 The call is replayed and listened to in full

© Cellcrypt 2010

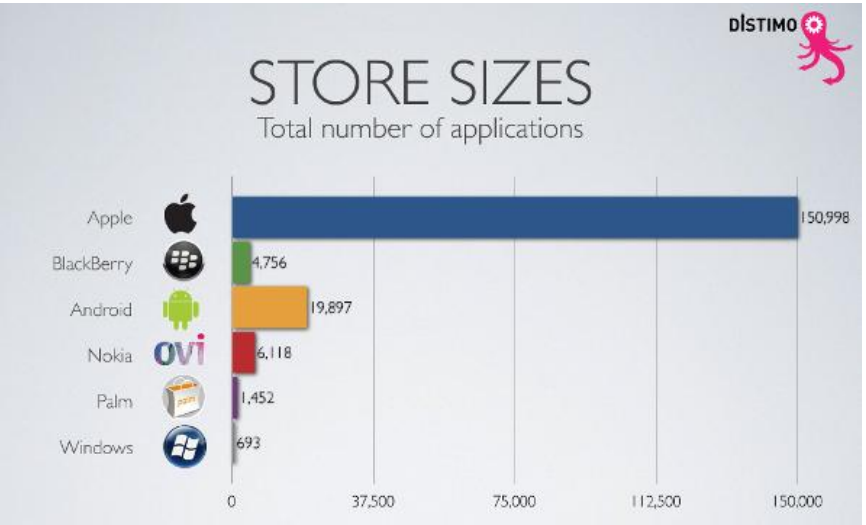
Mobile Phone Security Threats and Risks- Prosumer:

- **Evidence:**
  - **Blurring of lines**: Use of company-owned mobile phones for personal use and personal-owned mobile phones for company use ***(GI mSecurity Survey 65% of organisations allow employees to use personal phones for business use)***
  - **Who owns the data?** Legal issues, especially with Data Protection legislation, on who owns the data and who is responsible for protecting it
  - **Who is responsible for securing the mobile phones?**
  - **Can you install company security technology on a personal-owned device that is being used for business purposes?**

- **GI View:** ***Organisations need to set clear and usable policies that cover both company and employee-owned devices and ensure that appropriate technology controls are deployed***

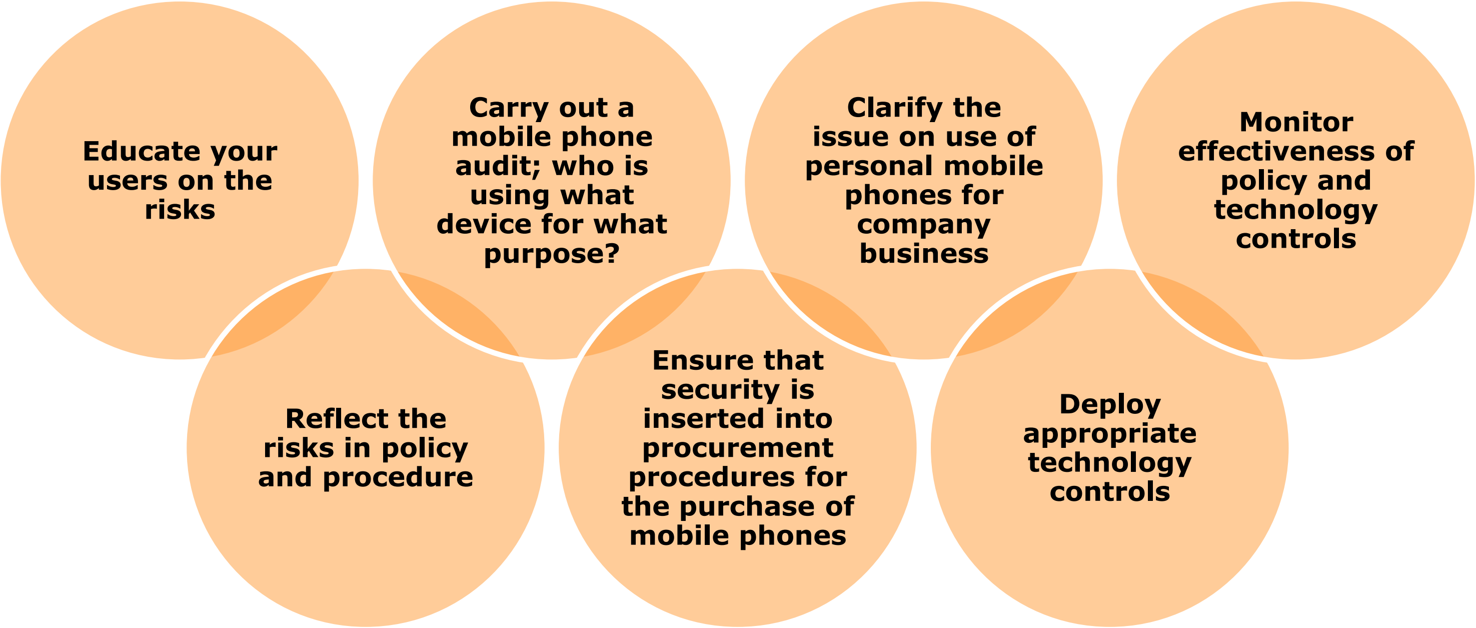
Mobile Phone Security Threats and Risks- App Stores:

Mobile App Store Sizes (February 2010)



- Evidence:
  - Apple App Store has seen over 2billion application downloads in an 18 month period
  - Do you know what you are downloading and can you trust the content?
  - Google Android Marketplace reportedly withdrew an app as it reportedly contained malicious code (Droid009)
  - Limited or no code checks on apps in stores
  - Potential weakness in signed app model that Symbian uses

Mobile Phone Security – GI Recommendations:



Educate your users on the risks

Carry out a mobile phone audit; who is using what device for what purpose?

Clarify the issue on use of personal mobile phones for company business

Monitor effectiveness of policy and technology controls

Reflect the risks in policy and procedure

Ensure that security is inserted into procurement procedures for the purchase of mobile phones

Deploy appropriate technology controls

Summary of mSecurity products and services

Mobile 2FA:

- **SMS-based solutions: Signify – www.signify.net & SMS Passcode – www.smspasscode.com**
- **OTP soft tokens: FireID – www.fireid.com & CRYPTOCard – www.cryptocard.com**
- **Voice solutions: PhoneFactor – www.phonefactor.com**
- **Mobile PKI: Valimo – www.valimo.com**

Mobile Anti-Virus:

- **F-Secure – www.f-secure.com (includes anti-theft) & SOPHOS – www.sophos.com**

Mobile Data Encryption and DLP:

- **Credant – www.credant.com & DeviceLock – www.devicelock.com**

Mobile Voice Encryption:

- **Cellcrypt – www.cellcrypt.com & Gold Lock – www.goldlock.com**

Want to find out more?

- Download the full survey findings and analysis: www.goodeintelligence.com (parts one and two are available now, parts three to be published April 2010)

- Contact alan.goode@goodeintelligence.com

- Follow us on Twitter: *http://twitter.com/goodeintel*

Thank You!