Mobile Device Security Risks and Remediation Approaches

Raj Chaudhary, Principal, Crowe Horwath LLP

In-Depth Seminars – D11

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

CRISC

CGEIT

CISM

CISA

2013 Fall Conference – "Sail to Success"

Informal Poll

- What is your title/role?
  - Internal Audit
  - IT Audit
  - IT / Information Security

Agenda

- Mobile Device Definition
- Current Landscape
- Case Study Exercise
- Risks and Rewards
- Mobile Device Control Considerations
- Mobile Device Management Solutions

What are Mobile Devices?

- Mobile Media
- USB Storage Devices
- Media Players (iPods, MP3 players)
- Laptops
- Smart Phones (Android, Blackberry, iPhone, Windows Phone)
- Tablets (iPad, Nexus, Galaxy)
- Portable Digital Assistants (PDAs)

- Post-PC Devices
- The Post-PC era is a market trend involving a decline in the sales of personal computers in favor of post-PC devices.

Audience Poll

- What devices does your organization support?
  - Phones
    - Blackberry
    - iPhone
    - Android
    - Windows Mobile
- Tablets
  - iPad
  - Other

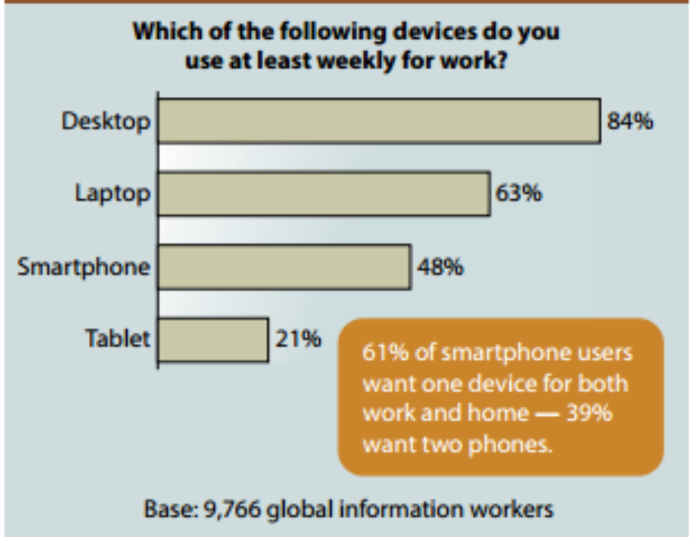
Audience Poll

- Does your organization have a Bring Your Own Device program?

The Mobile Device Challenge

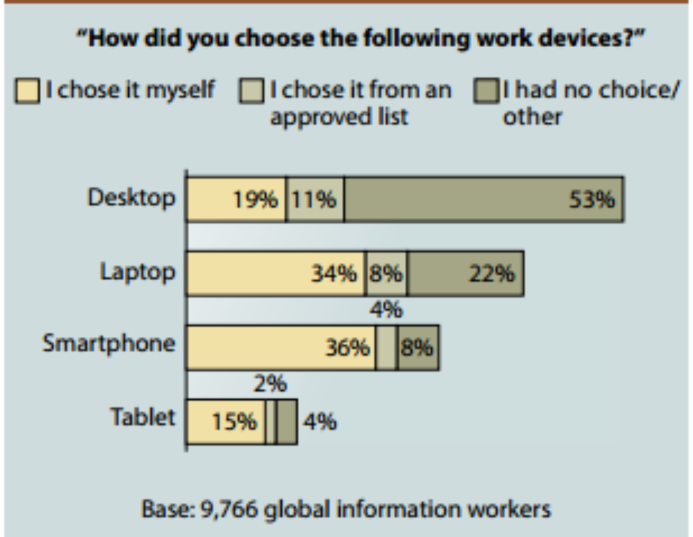
- Consumerization of IT
  - The shift of technology innovation is being driven by the consumer market as opposed to professional organizations. Advances in technology are introduced and adopted in consumer markets, and then are spread into the business.

2-1 Start With The Devices Used For Work

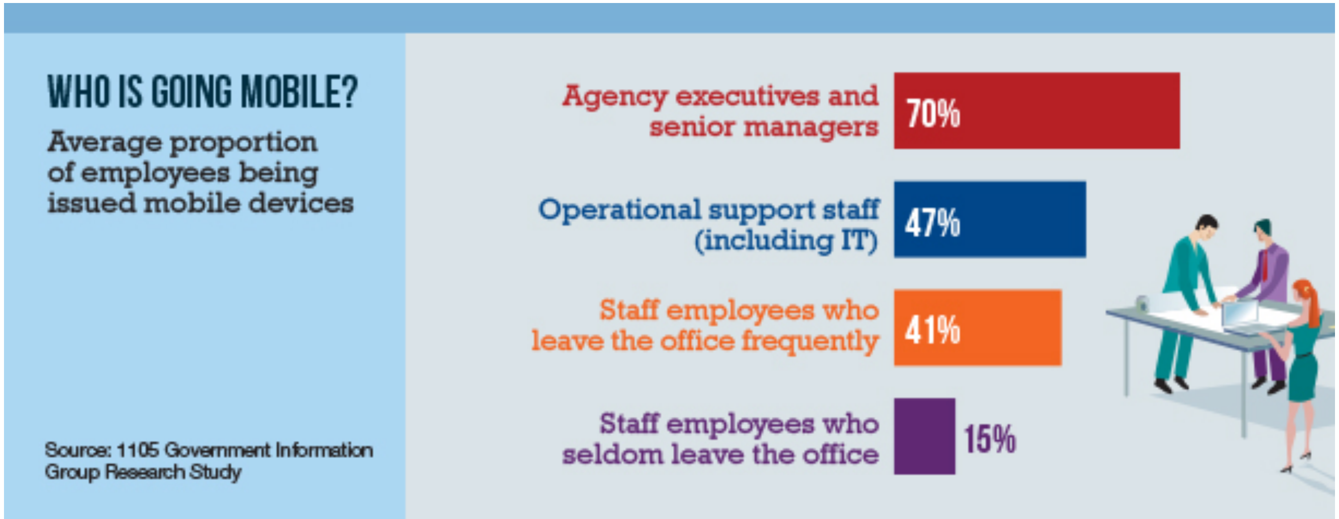


Base: 9,766 global information workers

2-2 Then Find Out Who Chose Their Own



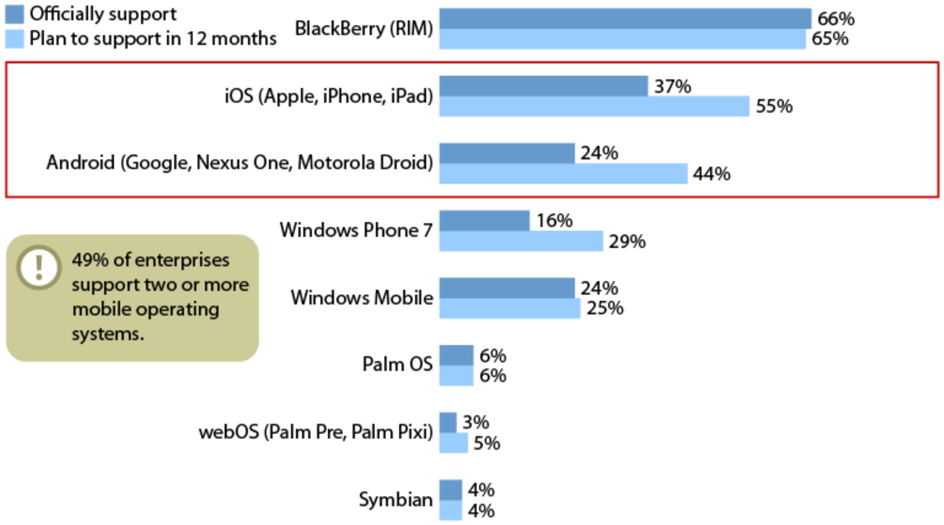
Base: 9,766 global information workers



Source: 1105 Government Information Group Research Study

What Can We Support Today?

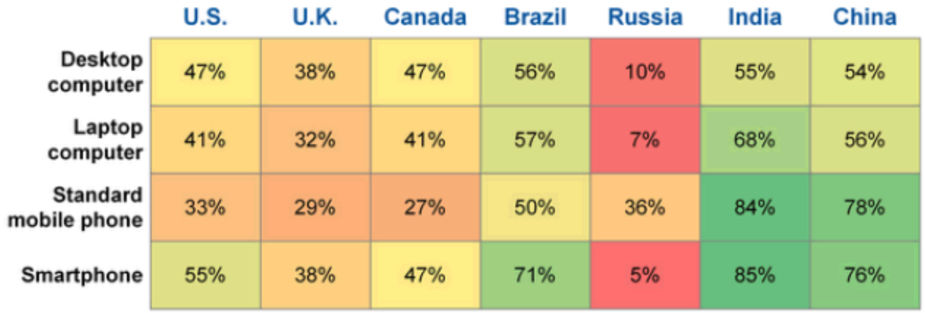
"To what extent does your firm's IT department currently officially support the following mobile operating systems?"



! 49% of enterprises support two or more mobile operating systems.

Base: 1,051 North American and European mobile technology decision-m

Source: Forrsights Networks And Telecommunications Survey, Q1 2011

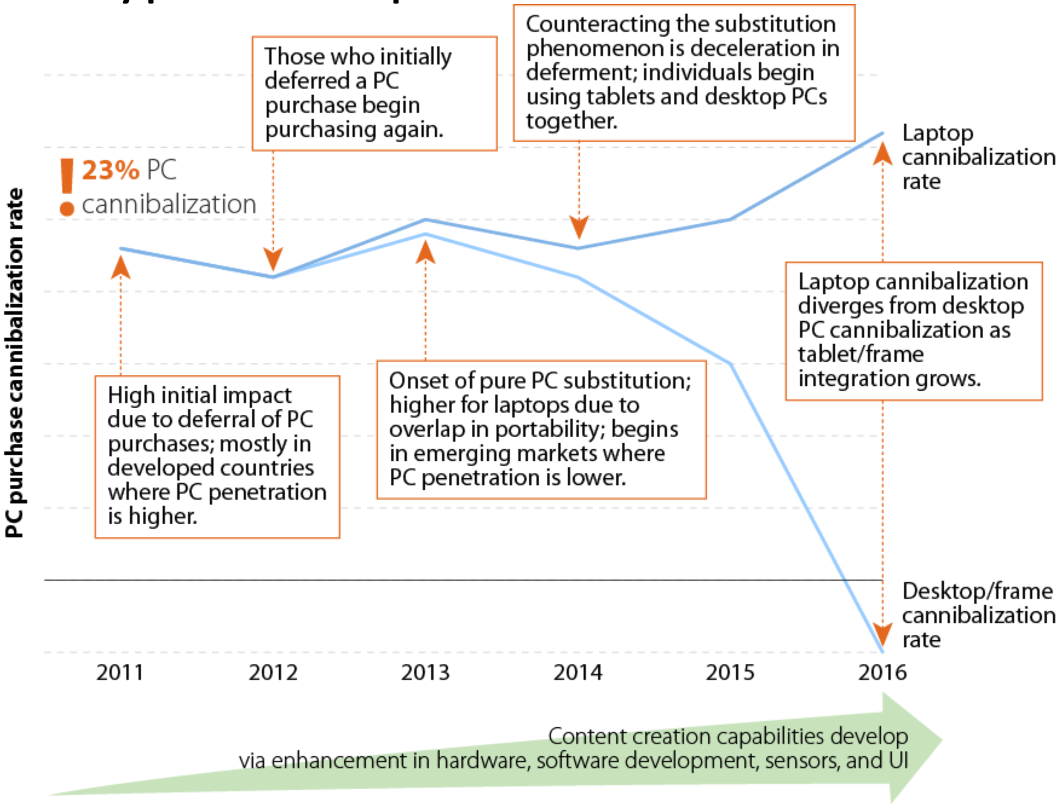


	U.S.	U.K.	Canada	Brazil	Russia	India	China
Desktop computer	47%	38%	47%	56%	10%	55%	54%
Laptop computer	41%	32%	41%	57%	7%	68%	56%
Standard mobile phone	33%	29%	27%	50%	36%	84%	78%
Smartphone	55%	38%	47%	71%	5%	85%	76%

Source: Gartner (April 2013)

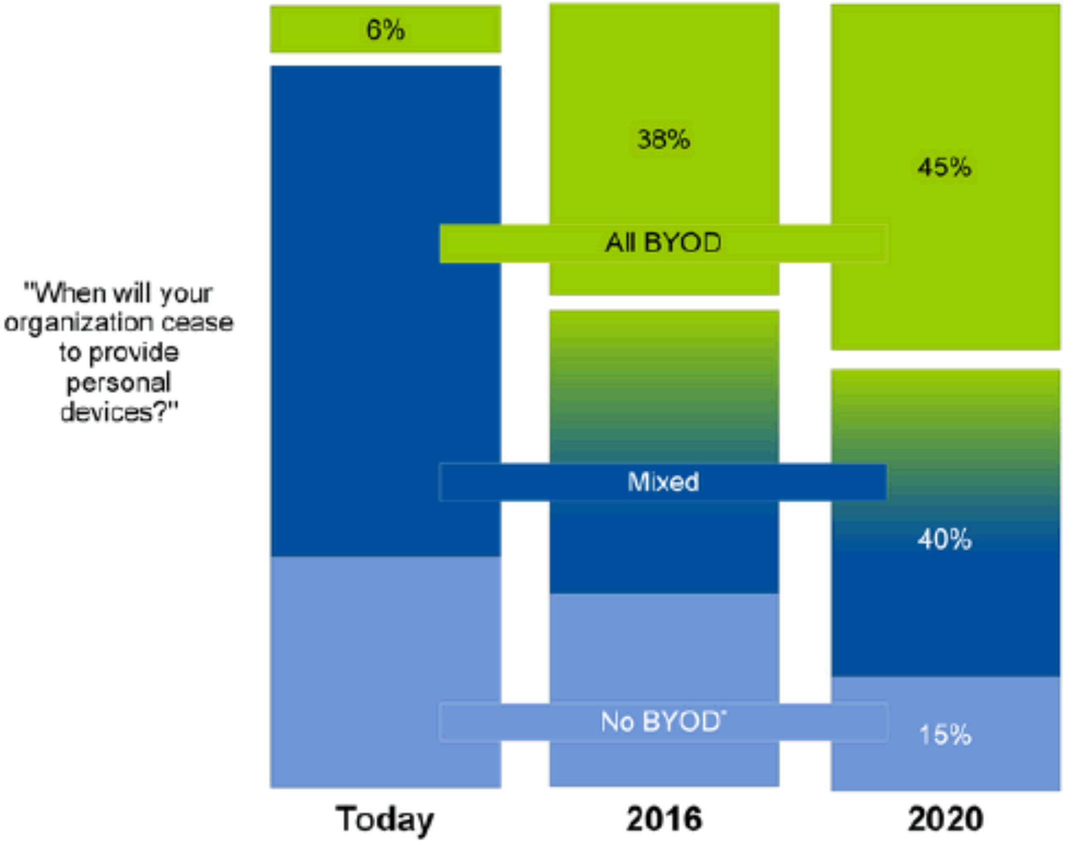
The Future of PCs…

- Many expect tablets and other mobile technologies to surpass the “typical” corporate issued PC.



Source: April 2012 “**Tablets Will Rule The Future Personal Computing Landscape**”

The Future of BYOD…

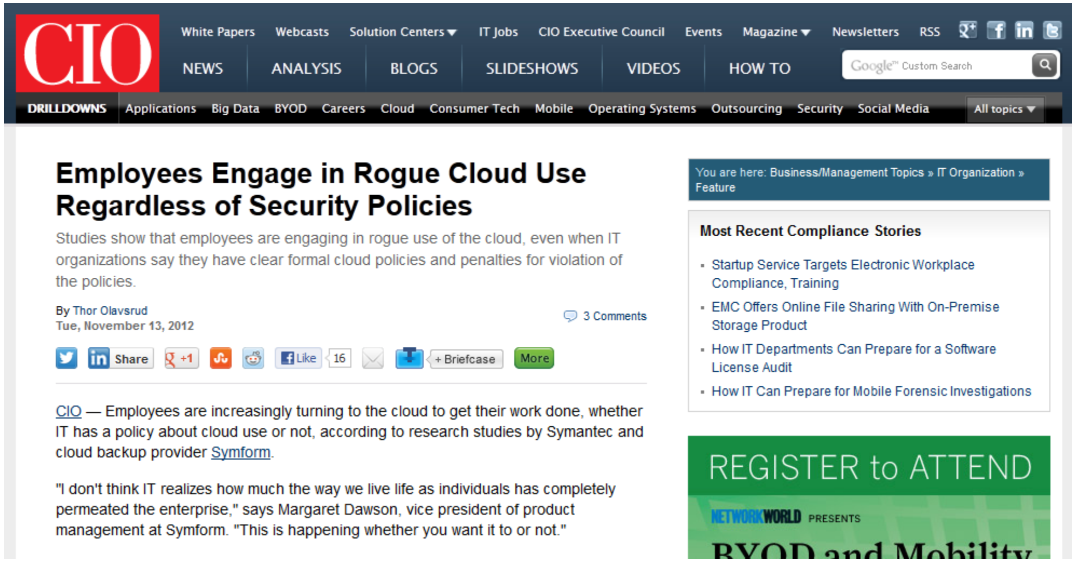


*Gartner analyst estimates; N = 2,053 worldwide

Source: Gartner (April 2013)

Where are Things Headed?

- Cloud storage is starting to be leveraged by employees for business data.
  - According to a study by Symantec, 69% percent of employees admit to rogue use of cloud-based email/communications, while 38% of employees admit to rogue use of cloud-based storage applications.



Employees Engage in Rogue Cloud Use Regardless of Security Policies

Studies show that employees are engaging in rogue use of the cloud, even when IT organizations say they have clear formal cloud policies and penalties for violation of the policies.

By Thor Olavsrud
Tue, November 13, 2012

3 Comments

CIO — Employees are increasingly turning to the cloud to get their work done, whether IT has a policy about cloud use or not, according to research studies by Symantec and cloud backup provider Symform.

"I don't think IT realizes how much the way we live life as individuals has completely permeated the enterprise," says Margaret Dawson, vice president of product management at Symform. "This is happening whether you want it to or not."

You are here: Business/Management Topics » IT Organization » Feature

Most Recent Compliance Stories

- Startup Service Targets Electronic Workplace Compliance, Training
- EMC Offers Online File Sharing With On-Premise Storage Product
- How IT Departments Can Prepare for a Software License Audit
- How IT Can Prepare for Mobile Forensic Investigations

REGISTER to ATTEND

NETWORKWORLD PRESENTS

BYOD and Mobility

CASE STUDY #1

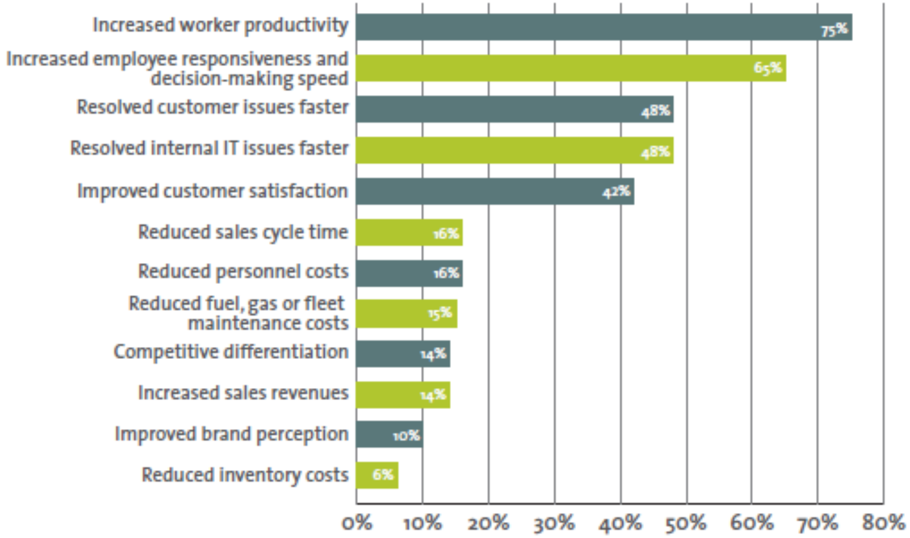
Case Study #1

- You are the President of a ten location car dealer with dealerships across California. You currently have a corporate policy for mobile devices, which provides a company owned phone for select C-level and upper management personnel at the dealership. Multiple Sales people have requested support for to use personal devices at the dealership, but to date those requests have been denied.
  - What are the risks you see the organization is facing based on the current environment?
  - What opportunities do you see for the organization, and how will you get there?
  - What challenges do you foresee in achieving the desired results?

RISK AND REWARD

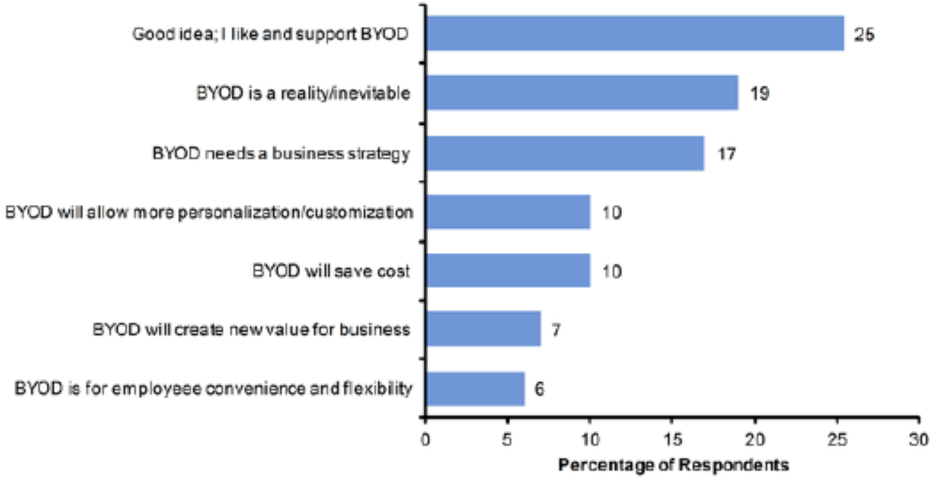
The Good…

- There are benefits of supporting the consumer mobile movement:
  - Productivity, Cost Reduction, Improved Sales, Improved Satisfaction



Base: 2,247 network and telecom decision-makers

Source: Forrester, *Enterprise and SMB Networks and Telecommunications Survey, North America and Europe*, Q1 2010



N = 374

Source: Gartner (April 2013)

Physical Risks

- There are risks with these new mobile technologies, and many organizations are unprepared to manage the risk comfortably.

- Physical Risks
  - Loss and Theft of Device
    - One mobile devices is stolen every 3 minutes[1]
  - Unauthorized access to an unlocked device

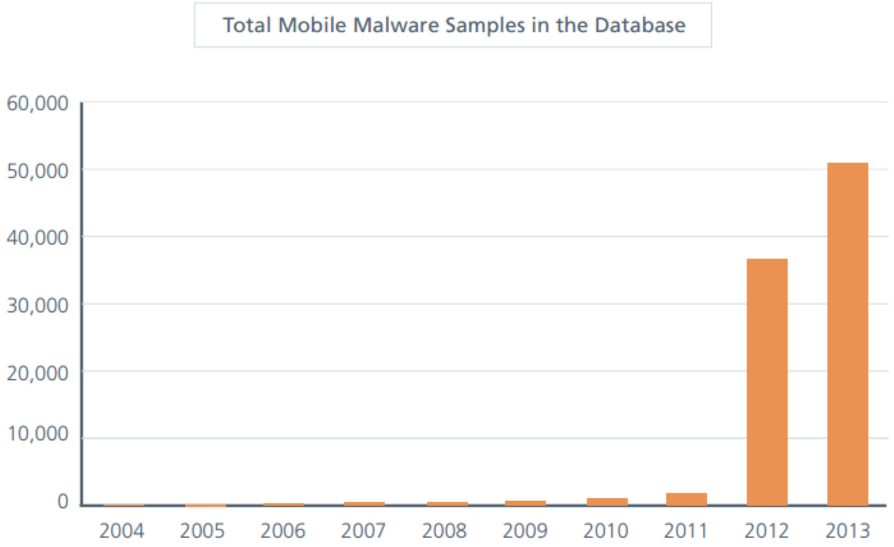
[1] http://news.bbc.co.uk/2/hi/uk_news/1748258.stm

Operational Risks

- Operational Risks
  - Consistency of reporting, wiping procedures
  - Lack of IT & end user training (use, security)
  - Data and device ownership (co-mingling of corporate and personal data)
  - Infringement on personal privacy (Legal Implications)

Operational Risks

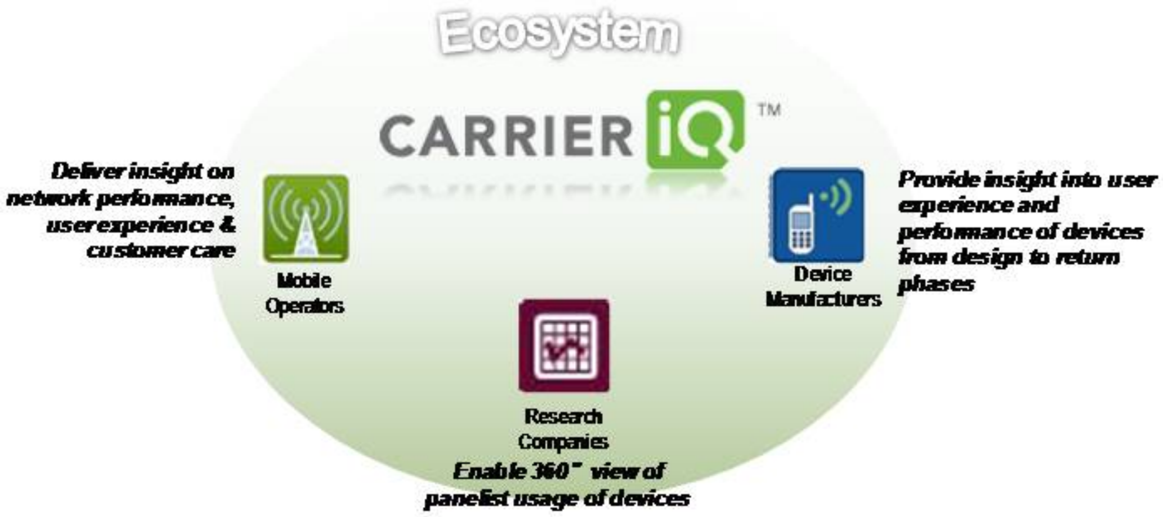
- Technical
  - Third party applications – Vulnerabilities or Malicious Software
  - “Jail broken” and “hacked” devices
  - Foreign networks (especially Wi-Fi)



Source: McAfee Threats Report - http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf

An Example of Risk in the Real world: Carrier IQ

- Application for smartphones which allegedly tracks users' activities
- 140 million devices
- Partner with Major Providers
- Controversy over what is tracked
- Do carriers have access to corporate data?



Ecosystem
CARRIER iQ™
Deliver insight on network performance, user experience & customer care
Mobile Operators
Device Manufacturers
Provide insight into user experience and performance of devices from design to return phases
Research Companies
Enable 360° view of panelist usage of devices

Mobile Device Breaches

- According to the U.S. Department of Health and Human Service published breaches of 500+, over 37,000 individuals' records have been compromised within the last year. All due to the loss or theft of a mobile device.

[1] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

MOBILE DEVICE CONTROL CONSIDERATIONS

Mobile Device Control Consideration Focus

- People
  - Awareness
    - Policies and Procedures / End User Responsibilities
    - Training
- Process
  - Request, Provisioning, and Management
  - Legal and Human Resources Considerations
- Technology
  - What technical controls should we consider?

People

- Awareness
  - Policies and Procedures / End User Responsibilities
  - Develop policies and procedures that employees are required to adhere to if they want corporate data on mobile devices (both corporate and personal)
  - These policies will be driven based on the planned usage, the organization's risk tolerance, and the mobile device management solution leveraged
- Training

Process

- Request, Provisioning, and Management
  - How will employees request access to corporate data?
  - How will the organization manage distribution of access when requested?
  - How will the organization track these requests?
  - If corporate devices are supported, how are these devices inventoried and tracked? Are there procedures to collect corporate devices when an employee leaves the organization?
  - Should a policy be distributed and signed prior to granting access?
  - How (or What) will the organization manage personal devices when there are issues?

Process

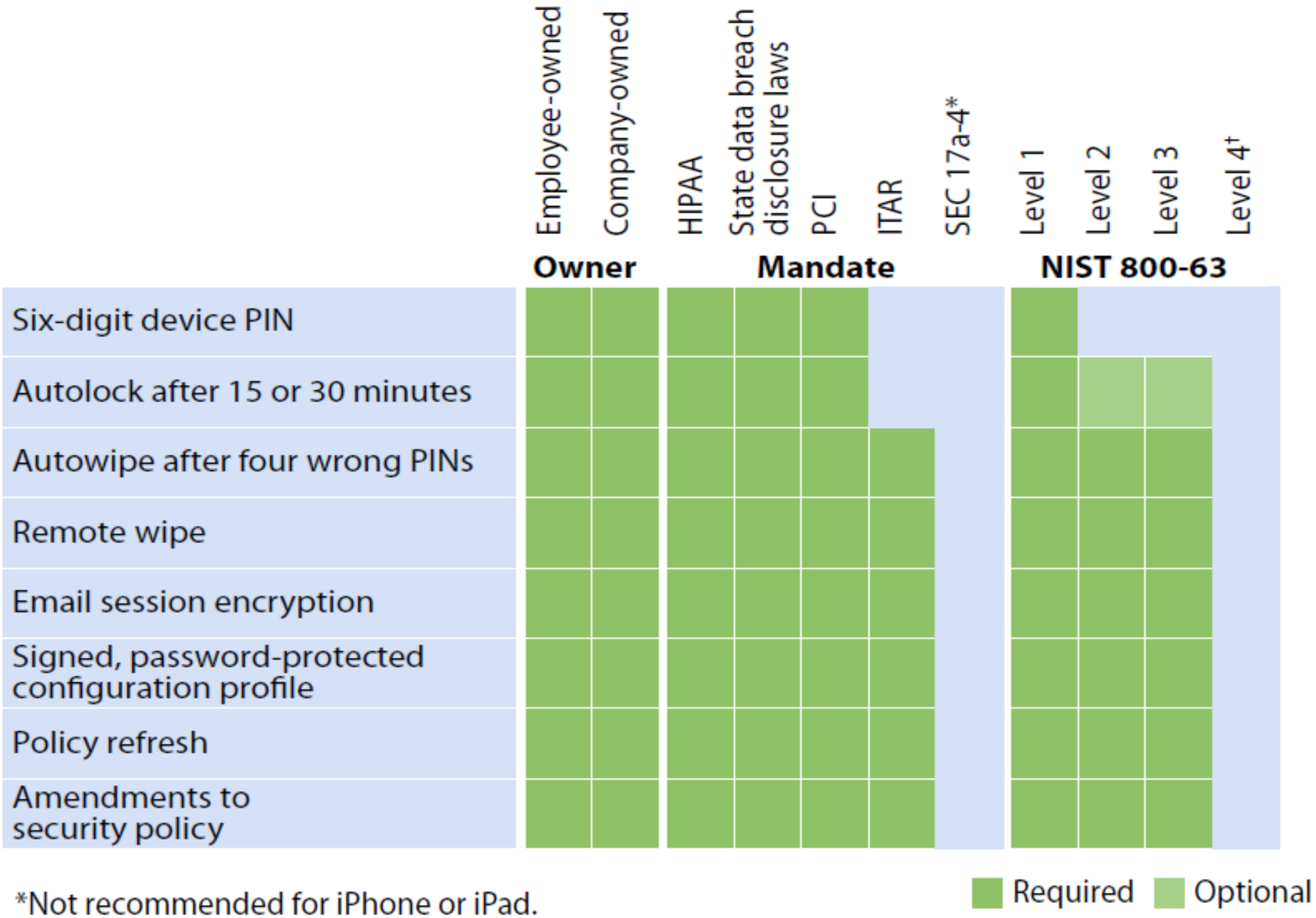
- Legal and Human Resource Considerations
  - There are various risks with mobile devices that the organization should discuss in order to determine the appropriate approach.
  - Update policies and training to communicate these policies to employees.

Technology Control Considerations

- Encrypt Data
  - Data (emails) sent to/from the device
  - Data stored on the device (hardware encryption) – Limited per OS

- Strong password controls
  - Passwords vs. PINs
- Auto-wipe after a set number of incorrect login attempts
- Lock device after period of inactivity
- Remotely wipe the data
- Authentication controls to corporate network

Technology Control Considerations



	Owner		Mandate					NIST 800-63			
	Employee-owned	Company-owned	HIPAA	State data breach disclosure laws	PCI	ITAR	SEC 17a-4*	Level 1	Level 2	Level 3	Level 4†
Six-digit device PIN	🟩	🟩	🟩	🟩	🟩			🟩			
Autolock after 15 or 30 minutes	🟩	🟩	🟩	🟩	🟩			🟩	▨	▨	
Autowipe after four wrong PINs	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	
Remote wipe	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	
Email session encryption	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	
Signed, password-protected configuration profile	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	
Policy refresh	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	
Amendments to security policy	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	

🟩 Required ▨ Optional

*Not recommended for iPhone or iPad.
†Not possible with iPhone or iPad.

Source: Forrester: August 2010

Technology Control Considerations

- Management/Deployment of Security Policies
  - Configuration Profiles
    - Signed
    - Password Protected
- Policy Refresh
  - Every time connects to server or predetermined "push"

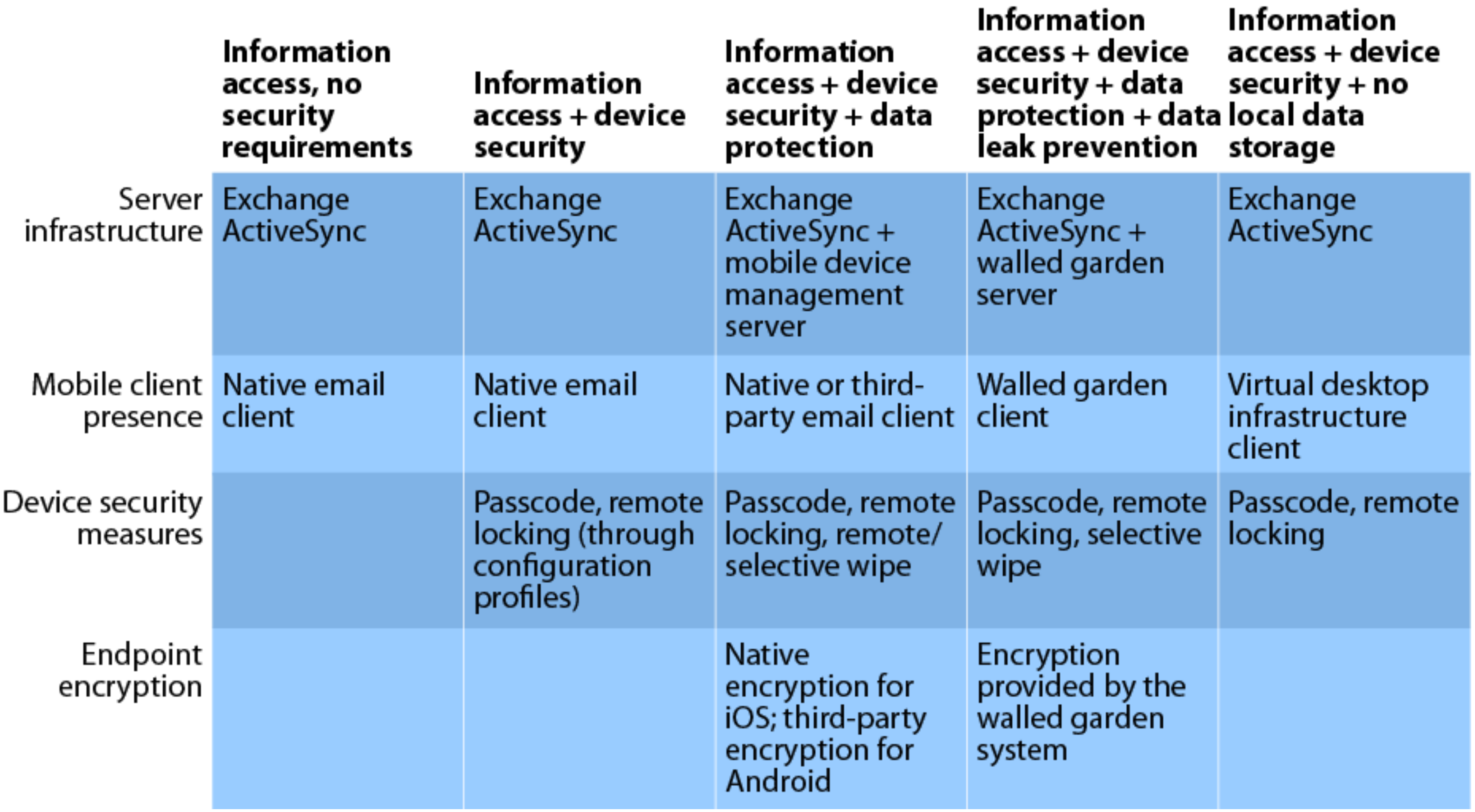
CASE STUDY #2

Case Study #2

- You are the Corporate Compliance Officer for a regional healthcare facility, including multiple hospitals and clinics. Your doctors have started bringing in iPads to help take notes and research when providing patient care. Currently only Blackberrys are supported by the business.
  - What are the risks you see the organization is facing based on the current environment?
  - What opportunities do you see for the organization, and how will you get there?
  - What challenges do you foresee in achieving the desired results?

MOBILE DEVICE TECHNOLOGY APPROACHES

Mobile Security and Risk Appetite



	Information access, no security requirements	Information access + device security	Information access + device security + data protection	Information access + device security + data protection + data leak prevention	Information access + device security + no local data storage
Server infrastructure	Exchange ActiveSync	Exchange ActiveSync	Exchange ActiveSync + mobile device management server	Exchange ActiveSync + walled garden server	Exchange ActiveSync
Mobile client presence	Native email client	Native email client	Native or third-party email client	Walled garden client	Virtual desktop infrastructure client
Device security measures		Passcode, remote locking (through configuration profiles)	Passcode, remote locking, remote/ selective wipe	Passcode, remote locking, selective wipe	Passcode, remote locking
Endpoint encryption			Native encryption for iOS; third-party encryption for Android	Encryption provided by the walled garden system	

MOBILE DEVICE MANAGEMENT SOLUTIONS

Mobile Device Management Solutions

- Mobile Device Management (MDM) Solutions help with:
  - Distribution of policies which control configuration settings
  - Monitoring
  - Control over applications

airwatch™

SAP®

SOPHOS

MaaS360® by Fiberlink

vmware®

Exchange

Good™

MobileIron®

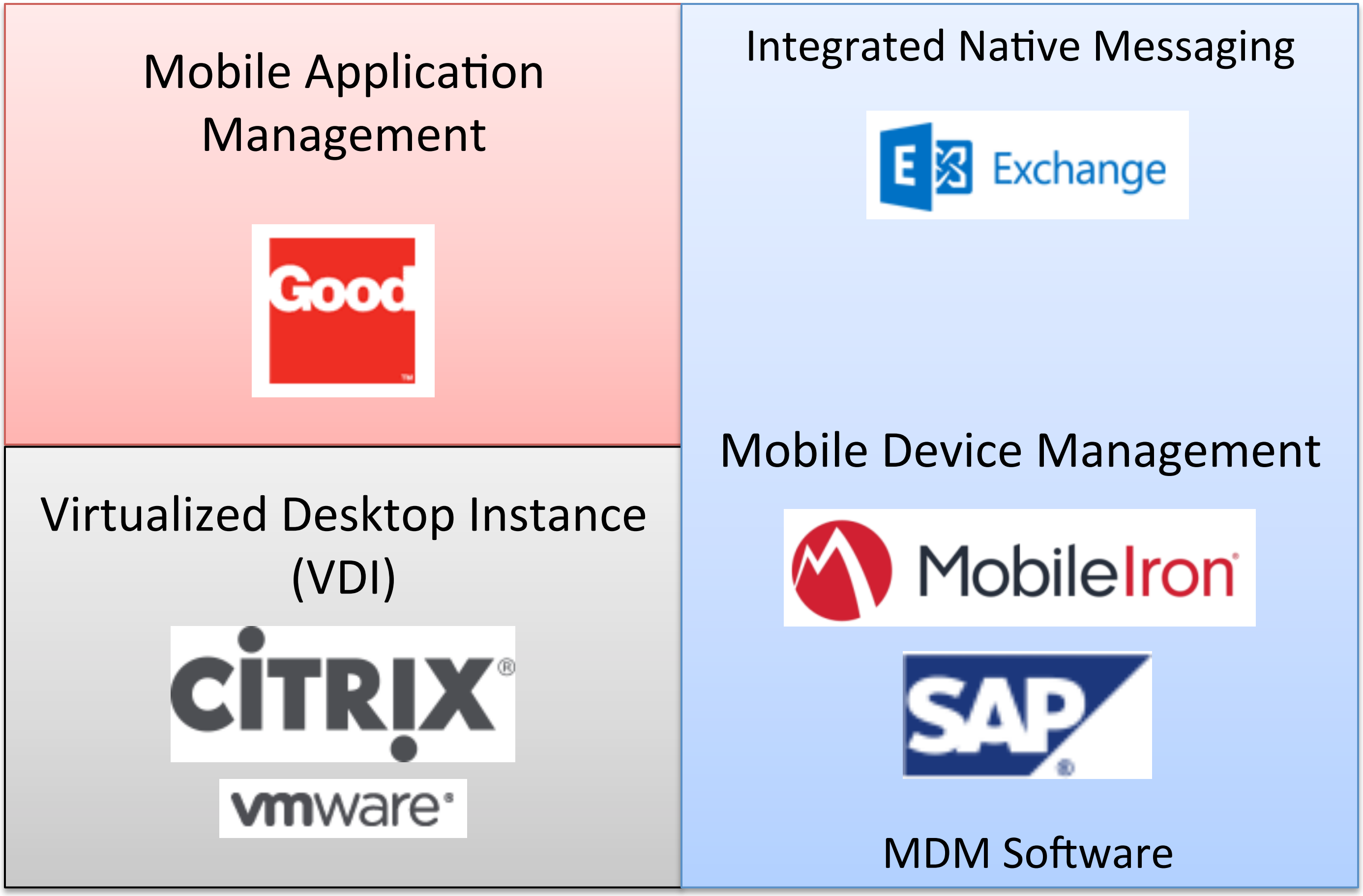
CiTRIX®

Mobile Device Management Solutions

- Gartner defines the elements of a Mobile Device Management (MDM) Solution as:
  - **Software management —** This is the ability to manage and support mobile applications, data and OSs.
  - **Network service management —** This is the ability to gain information off of the device that captures location, usage, and cellular and wireless LAN (WLAN) network information, using GPS technology. Network access control (NAC) features are also found here.
  - **Hardware management —** Beyond basic asset management, this includes device provisioning and support.
  - **Security management —** This is the enforcement and support of standard device and data security, authentication, and encryption. Application containerization, VPN and encryption software are also part of this capability.

Mobile Device Management Landscape: Market Analysis

- Large number of vendors, many niche players
  - Gartner Magic Quadrant Study (May 2013) identified 100+ companies in the space in some way
- Conclusions
  - Installation options include traditional management, SaaS onsite, SaaS cloud
  - The mobile device operating system/version may introduce limits to MDM functionality
  - Clear and custom reporting is critical
  - Solutions will continue to mature
- Magic Quadrant "Leaders"
  - AirWatch
  - MobileIron
  - Good Technology (GFE)
  - SAP Afaria
  - Citrix
  - Fiberlink



Mobile Application Management

Integrated Native Messaging

Mobile Device Management

MDM Software

Virtualized Desktop Instance (VDI)

Mobile Device Management – Integrated Solutions

How It Works

- Use your existing mail platform and its functionality to control mobile devices
- Mail typically is delivered to the native mail client on the device
- Configuration Profile is deployed to set security policies

Pros

- Lower cost: Makes use of existing software infrastructure
- IT may have a greater familiarity with existing mail platform
- User experience – no need to open a separate app to get to corporate data

Cons

- Security policy enforcement can be circumvented
- Limited Functionality: Email/Messaging data only (Mail, Contacts, Calendar)
- Corporate and Personal data may be comingled
- Less protection against jailbroken phones/Can be duped

Examples

Exchange

Mobile Device Management – MDM Software

How It Works

- 3rd Party software provide control of whole mobile device
- Typically pushes security policies through an agent
- Delivers mail to native client

Pros

- User experience – no need to open a separate app to get to corporate functionality
- Additional functionality to deploy applications, Intranet etc.
- Provides management console, reporting to track and manage devices
- Provides increased security controls, granularity of control

Cons

- Requires new infrastructure & software, additional cost
- Corporate and personal data may be comingled
- Relies somewhat on the security of the phone itself
- Potential Device performance impact

Examples

MobileIron

SAP

Mobile Device Management – Application Control

How It Works

- Client installed on the mobile device creates a sandbox or segment for corporate data and applications
- Relies on application controls rather than device controls - Requires a separate username and password to access this application

Pros

- Does not rely on the security of the device
- Ability to manage and eventually wipe just corporate data
- Provides management console, reporting to track and manage devices

Cons

- Requires new Infrastructure & software, additional cost
- User experience will be impacted, need to open separate application
- Potential limit on deployment of non-web corporate applications

Examples

Good™

Mobile Device Management – Application Control

How It Works

- Application installed on device allows connection to remote desktop environment
- No security policies are set – "Thin Client" model
- Encrypted access to desktops and applications

Pros

- Desktop functionality and additional flexibility for app deployment
- Lower Overhead for IT Management

Cons

- Requires new software, may require new Infrastructure
- Desktop User experience for phones, small devices
- Limited (if any) offline functionality

Examples

CITRIX®

vmware®

CASE STUDY #3

Case Study #3

- You are the Chief Technology Officer of a start-up technology company that strives on the employee experience. Instead of providing employees with a computer, you decide to provide each employee $2,000 to purchase their own devices for corporate use, including laptops, phones, and tablets.
  - What are the risks you see the organization is facing based on the current environment?
  - How would you secure the devices and data?

Q&A: OPEN DISCUSSION