

# BYOD(evice) without BYOI(nsecurity)

**Dan Houser CISSP-ISSAP CISM**  
**Goran Avramov MCSE+M VCP4**  
**Cardinal Health**



Session ID: HOT-107

Session Classification: Intermediate

**RSACONFERENCE2012**

# Agenda

- Drivers for Bring Your Own Device (BYOD)
  - Industry
  - Cardinal Health business
- Current state
- BYOD implementation
  - Vision
  - Security guiding principles
  - Approach and timeline
  - Lessons learned

# Cardinal Health

- Leading provider of products and services across the healthcare supply chain
- Extensive footprint across multiple channels
- Serving >40,000 customers with renewed focus
- Approximately 30,000 employees with direct operations in 10 countries
- >\$103B FY11 pro forma revenue\*
- Number 19 on the Fortune 500 list



Broadest view of the healthcare supply chain

# Changing Industry & Consumerization

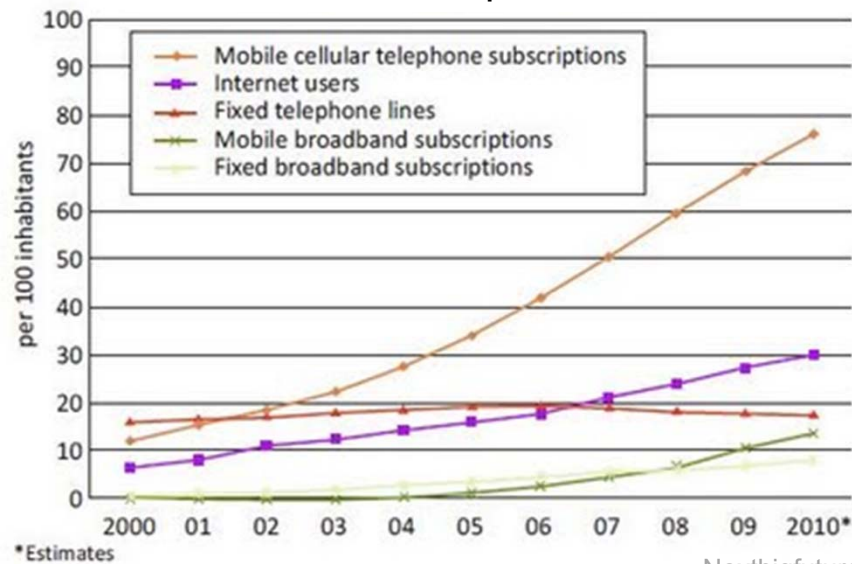
Estimated 10 billion smart phones by 2014

Android & iOS sales brisk over last 2 years

Consumers now largest computing purchaser

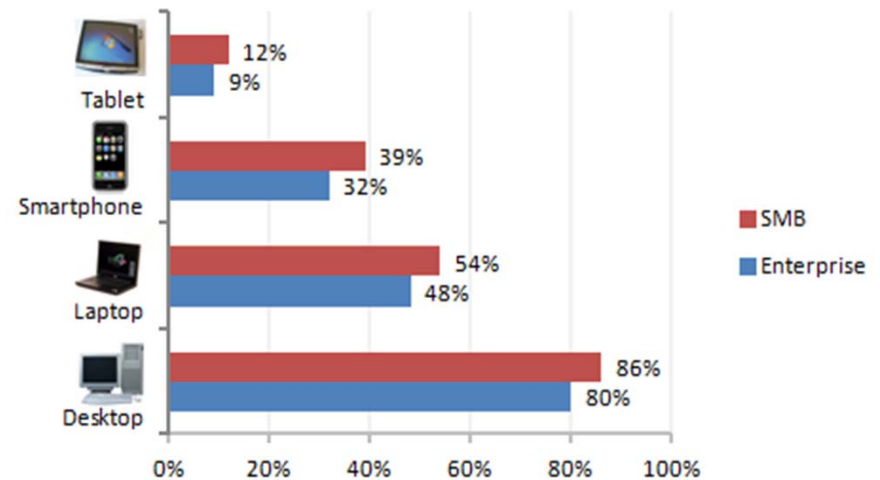
Consumerization impacts business environs

Global ICT development, 2000-2010



Nextbigfuture.com

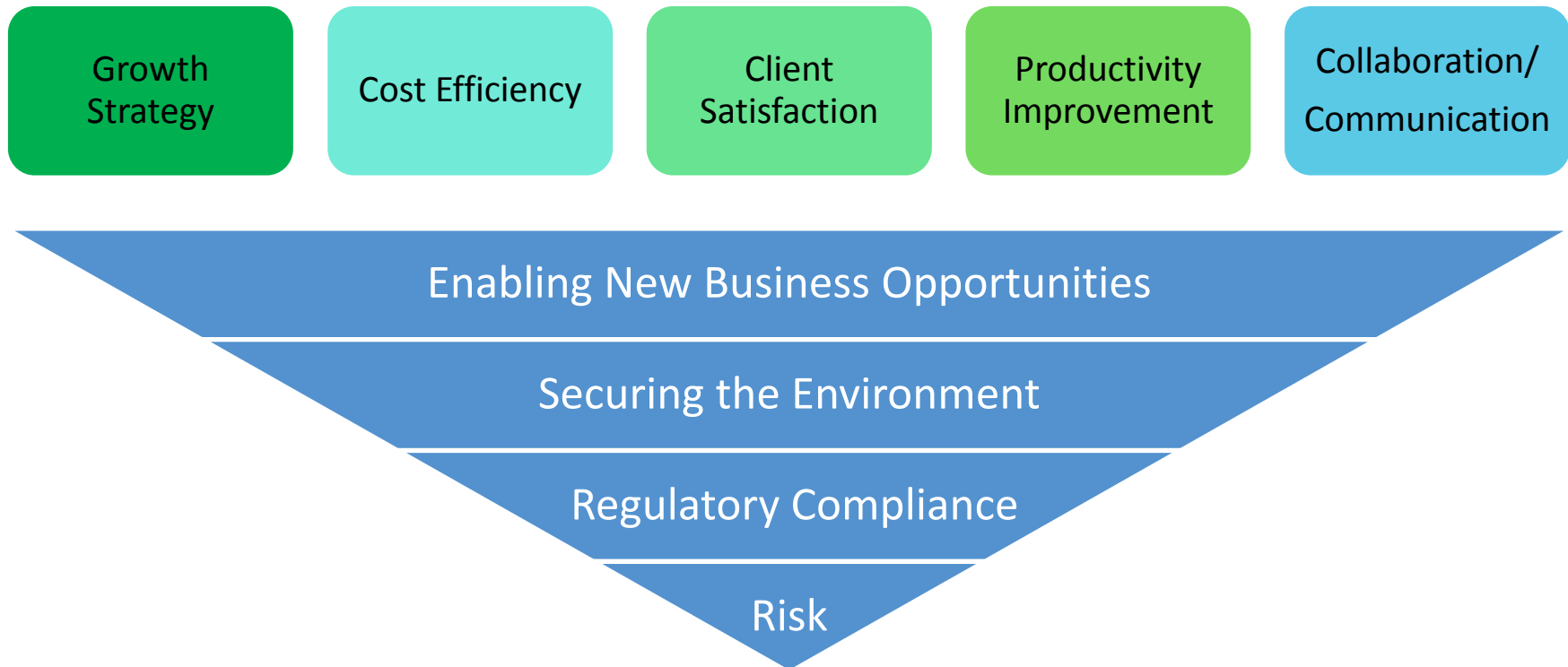
What devices do you use for work?



Source: Forrester Q2 2011 US Workforce Technology & Engagement Survey



# Business Drivers To Change



## Call to Action

# Stakeholders in the Mobile Device Environment

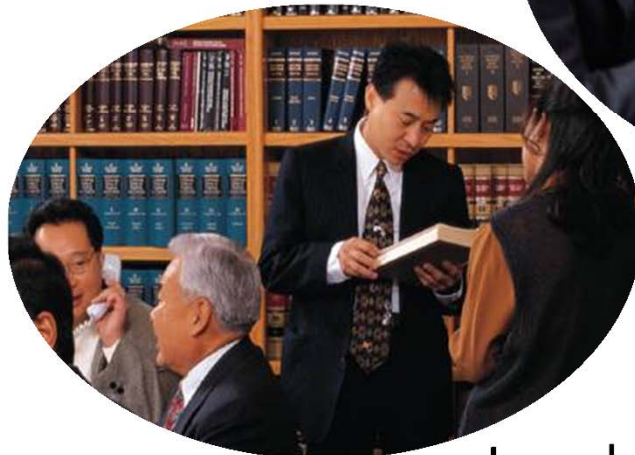


Mobile  
Worker

Gen Net



CFO/CIO

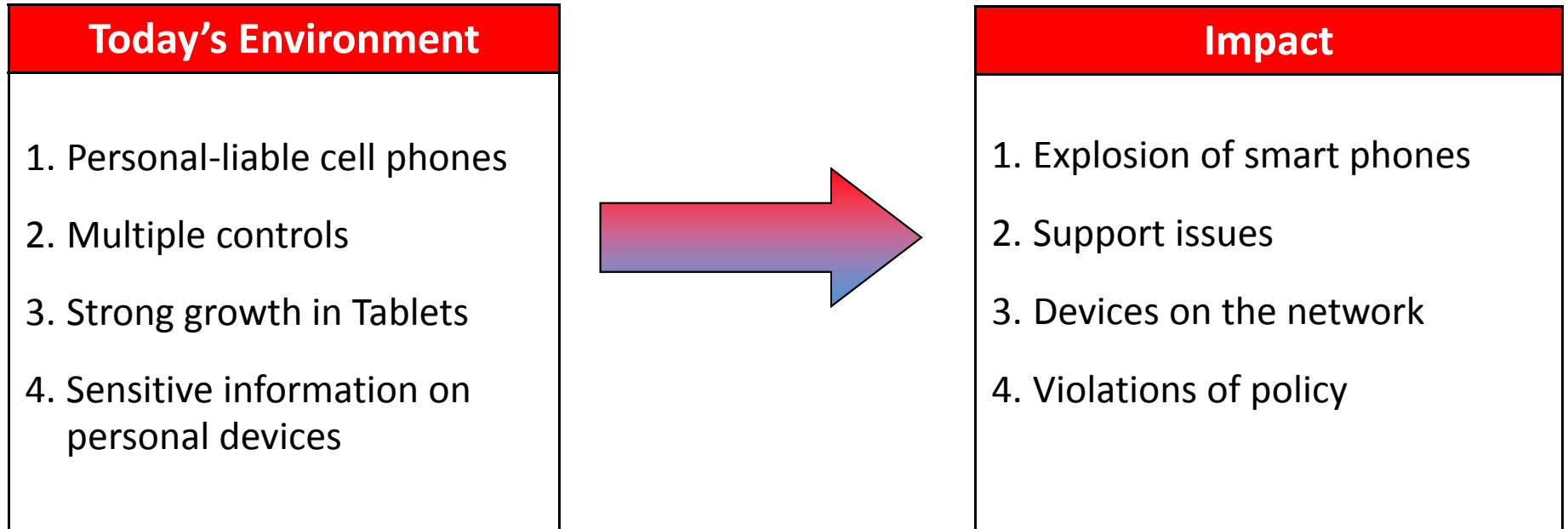


Legal



Knowledge Worker

# Cardinal Health SmartPhone Environment



Today's Controls	
1. Personal device waivers	4. Password screensaver enforcement
2. Remote wipe	5. Excessive password retry ⇒ Wipe
3. Device level encryption	6. Some monitoring controls

***Will our controls support the future needs?***

## VDI & BYOD Vision

Leverage the  
benefits of  
new  
technology

- Provide greater device flexibility and choice
- Reduce Cardinal Health's total cost of ownership
- Support a mobile workforce – application access, anywhere, anytime, anyplace
- Embrace consumerization of IT, leverage new strategies for optimizing employee productivity
- Transition to self-service model
- Improve security through centralized data control, patching and upgrades

## VDI & BYOD Principles

### Improve Security

- Personal devices will not have the ability to **download and save** Cardinal Health information
- Personal devices will not have **direct access** to Cardinal Health's internal network
- **Security controls** will be implemented in the Cardinal Health environment to minimize impact to personal devices
- Local **email archives** (.pst files) will not be allowed within the virtual environment

# Cardinal Health's Approach to BYOD(evice)

IT-developed Vision and Principles

Desktop – Server – Architecture – Security – Network

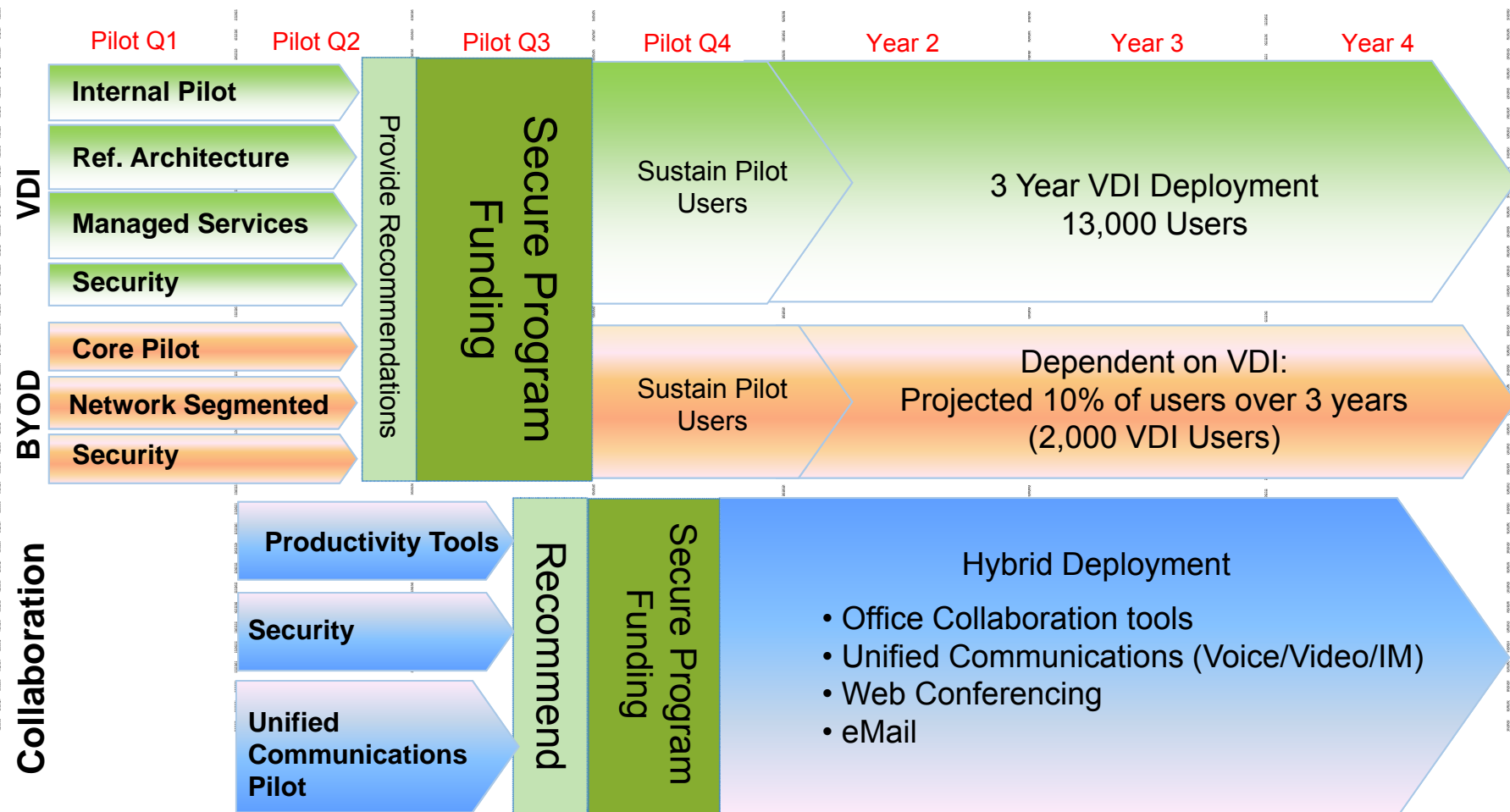
Security solutions built into the program

A program level approach that includes all non-company owned devices (today and tomorrow)

A common platform to support those devices

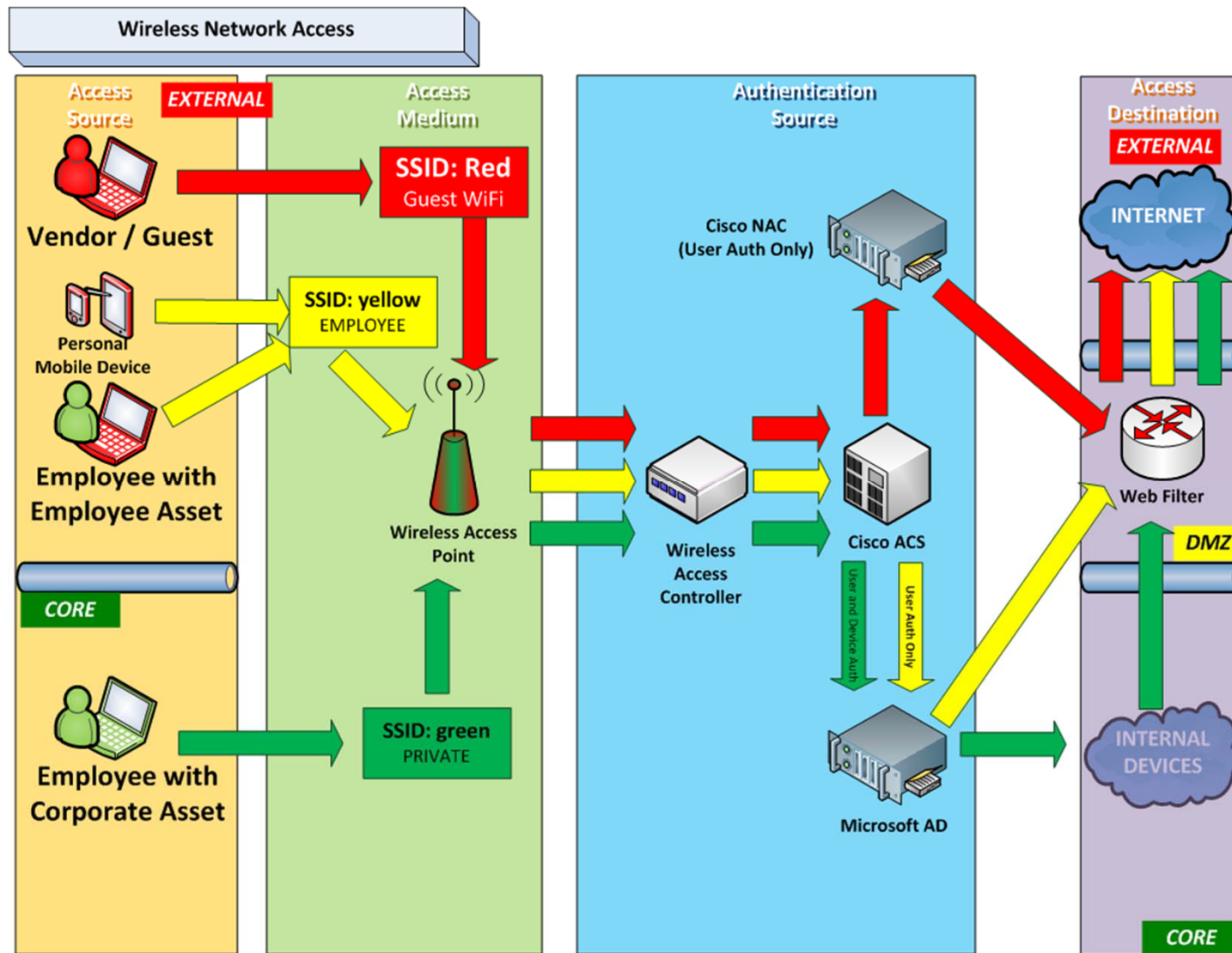
BYOD:

# Program Roadmap and Timeline





# Segmentation of BYOD Traffic





# The Journey Isn't Complete Yet...

Work in  
Process

- End user acceptance
- Business involvement
- Subsidy to employees
- Worker segmentation
- Expansion & Maturity of DLP
- Mobile application delivery
- Partitioning of corporate and personal data

# Application

- Build a collaborative approach with Business, Legal, Infrastructure, Risk & Architecture
- Identify user segmentation
  - Geographical
  - Role
  - Common Applications
- Virtualize / isolate applications
- Security
  - Revisit policies, particularly User Access Policy
  - DLP & information classification
  - Segmentation
- Senior leadership support to overcome resistance
- Realistic expectations – VDI / BYOD is NOT one size fits all



# CardinalHealth

*Essential to care*



Goran.Avramov@cardinalhealth.com

Dan.Houser@cardinalhealth.com

Portions © Copyright 2012, Cardinal Health, Inc. or one of its subsidiaries. All rights reserved.

**RSACONFERENCE2012**

# Cisco's BYOD Strategy & Deployment 2012

Nasrin Rezai  
CTO Security  
WW Security Architectures



Session ID: HOT-107

Session Classification: Intermediate

**RSA** CONFERENCE 2012

# My Goals For This Session...

## Cisco-on-Cisco

- Cisco IT Security Strategy
- BYOD Journey - Lessons Learned

# Cisco IT Strategy

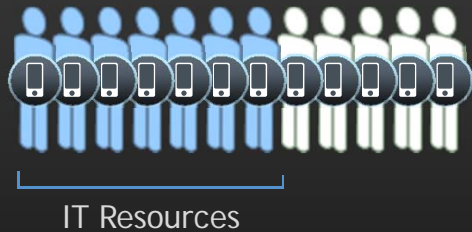


**RSA**CONFERENCE**2012**

# Market Transitions

7 Billion New  
Wireless Devices  
by 2015

Mobile Devices



MOBILITY

Blurring  
the Borders

Consumer ↔ Workforce  
Employee ↔ Partner  
Physical ↔ Virtual



WORKPLACE  
EXPERIENCE

Changing the  
Way We Work

Video projected to  
quadruple IP traffic by 2014  
to 767 exabytes



VIDEO

# Security Trends & Opportunities for Cisco IT

## External

**Social networking**  
(virtual "friends")

**Sophisticated Cyber attacks**  
(Advance Persistent Threats)

**Cloud, XaaS**  
(disappearing perimeter)

## Workforce

**Who I work with**  
(Collaborative IP Protection)

**What I use to work**  
(end point identification)

**Where I work from**  
(location awareness)

## Growth

- Product Strategy Accelerator
  - Cisco-on-Cisco Success
    - Product Direction
  - Best Practice Leadership
- Securely Enable NBM's
  - I/PaaS Offerings
  - New revenue streams
  - COGS Mindset





# Pervasive Security Accelerator - V



CIO / CSO

"Cisco is secure. We will not get compromised in the marketplace. We can secure our services without slowing down my client business. We are ready because we embraced security."

"Security does not get in the way of doing my business. I know what is expected from me."



Employee

"I am responsible for the security of my service, and able to make data-driven decisions"



Service Owner

"I know how to leverage the security capabilities needed to protect my service"



Service Architect

"We know what threats and data patterns to monitor, and how to respond"



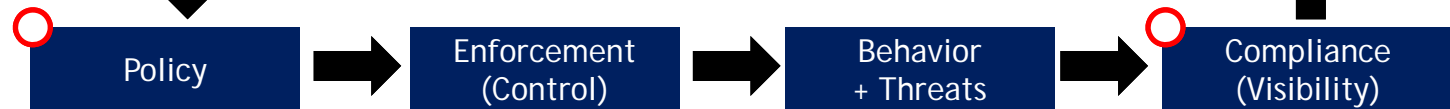
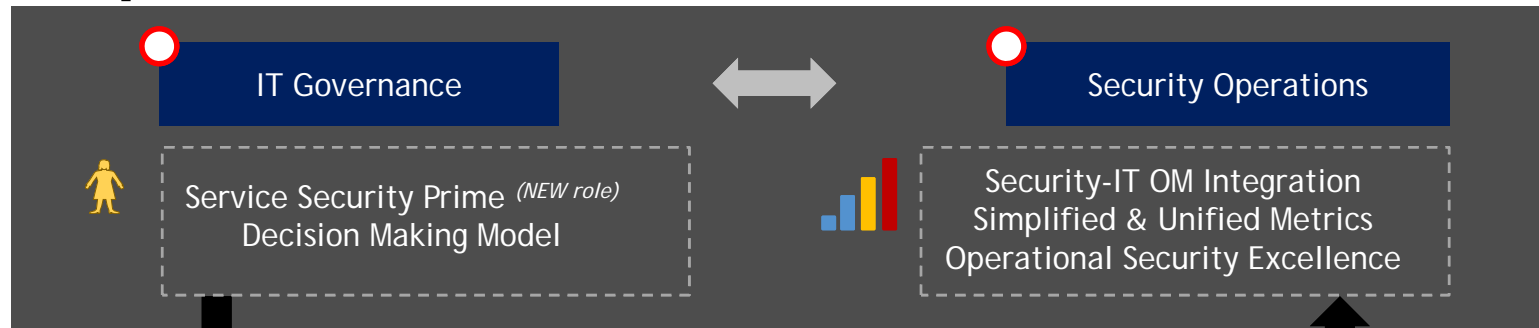
Security Operations



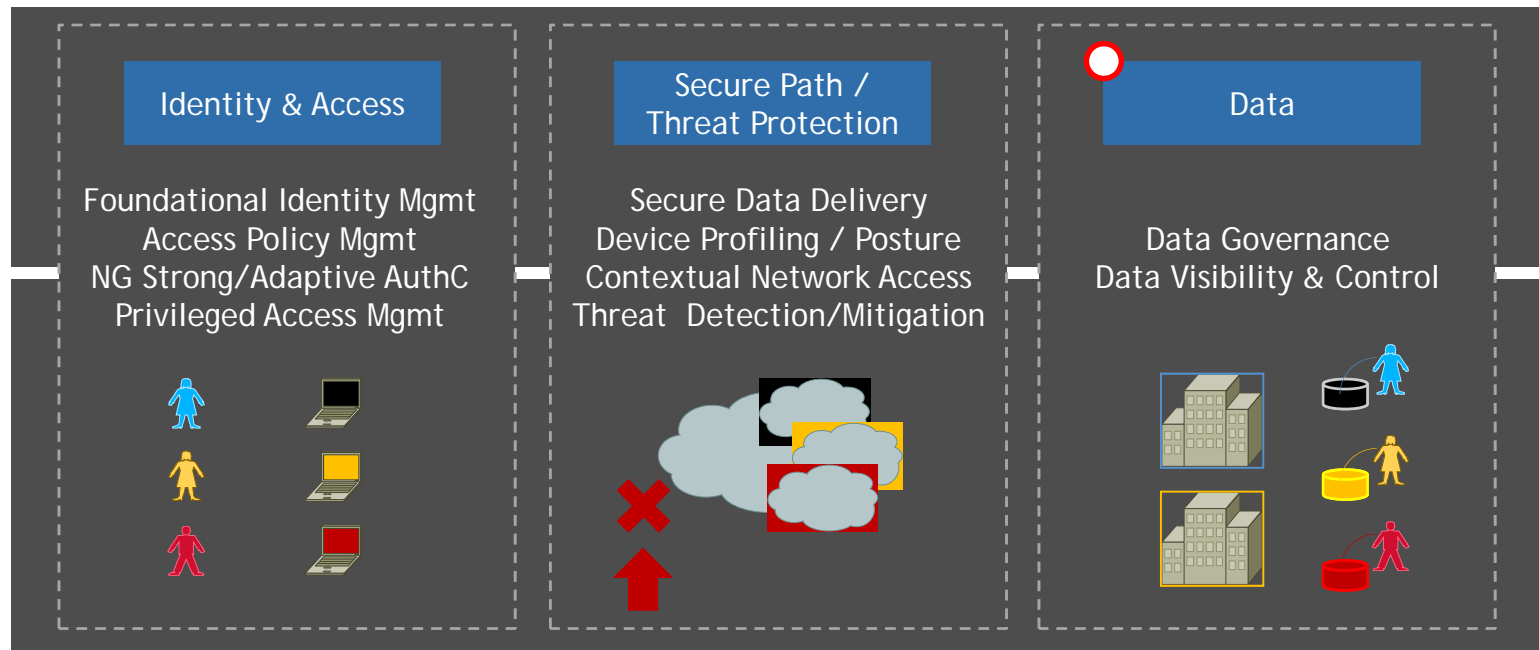
# PSA : Top-Level Architecture View

○ Highly Transformational  
Architecture Focus Areas  
for PSA

Governance  
Plane



Management  
Plane







Data  
Plane



# BYOD...Cloud

## 1. Tight Access Controls & Trust

Access Entitlement

Identity & location	Untrusted Device	Trusted Device	VDI
 Guest	✗	✗	✗
 Vendor	✗	✗	✓
 HRE	✗	✗	✓
 Employee	✗	✓	✓

## 2. Segment Services in DC (TrustSec)

Public data  
Sensitive data  
data

## 4. Enforce in the network

Guest (ISE)  
Access (Default)

VXI Only

Trusted Device or VXI

## 3. Manage through Policy (ISE)

# Cisco IT BYOD Journey

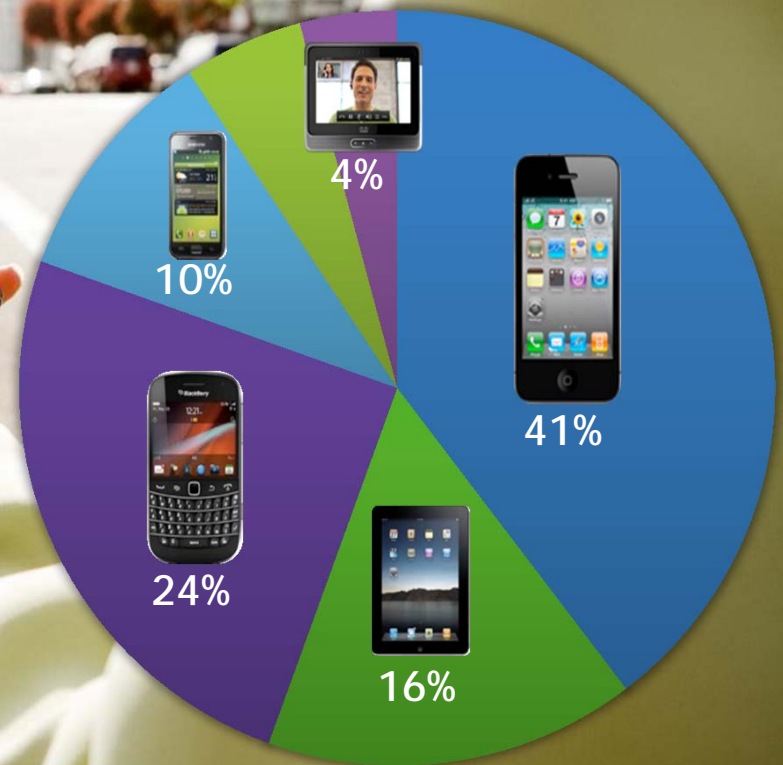


**RSA CONFERENCE 2012**

# BYOD Mobile Landscape

Platform	Dec 2009	Dec 2010	Dec 2011
iPhone	2,266 9%	10,662 32%	20,581 41%
iPad	0 0%	1,822 6%	8,144 16%
BlackBerry	13,611 53%	15,188 46%	12,290 24%
Android	0 0%	1,390 4%	5,234 10%
Others	9,647 38%	4,292 12%	2,185 5%
Cisco Cius	0 0%	0 0%	2,104 4%
Total	25,524	33,354	50,538

Smartphones and Tablets at Cisco









Cisco's total mobile device count grew 52% in 12 months.





# CISCO BYOD Deployment Strategy

	Trusted Platforms				Untrusted Platforms	
	IT Managed 	IT Virtual Machine 	Apple Mac laptop / tablet 	Mobile Devices / Tablets 	BYOD / Any PC device 	Mobile Devices / Tablets 
<b>IT Services</b>						
Help Desk Support	Yes	Yes	No	Yes	No	No
Email	Yes	Yes	Yes	Yes	Yes	Yes
Corporate Access (Apps, print, etc.)	Yes	Yes	Yes	Yes	Limited	Limited
Registered / Accounted For	Yes	Yes	Yes	Yes	No	No
<b>Network</b>						
User attribution (customer tools, 8021x, TrustSec)	Yes	Yes	Yes	Yes	Yes	Yes
Policy Enforcement Wired/Wireless / Remote (ISE)	Yes	Yes	Yes	Yes	Yes	Yes
Malware (WSA, ESA)- On Network	Yes	Yes	Yes	Yes	Yes	Yes
Security Monitoring - On Network	Yes	Yes	Yes	Yes	Yes	Yes
Direct Network Access	Yes	Yes	Yes	Yes	Limited / VDI	Limited / VDI
VPN (AnyConnect)	Yes	Yes	Yes	Yes	Limited	Limited
ScanSafe	Yes	Yes	Yes	Yes	Yes	Yes
<b>Device</b>						
AV/SPAM	Yes	Yes	As Capable	As Capable	As capable	As Capable
Patch Management	Yes	Yes	Yes	Yes	Yes	No
CSA/HIPS	Yes	Yes	Yes	No	Yes	No
Password Protected	Yes	Yes	Yes	Yes	Yes	No
Encryption/Remote Wipe/Asset Management	Yes	Yes	Yes	Yes	No	No
Device Identity/Certificate	Yes	Yes	Yes	Yes	Yes	Yes
Device Authentication (TrustSec, ISE)	Yes	Yes	Yes	Yes	No	No
User Authentication (TrustSec, ISE)	Yes	Yes	Yes	Yes	Yes	Yes
<b>Application</b>						
App store , application virtualization	Yes	Yes	Yes	Yes	No	No
Mobile App Development & Security	Yes	Yes	Yes	Yes	No	No
<b>Data /Policy/Process</b>						
Secure Data Storage (on device)	Yes	Yes	Yes	Yes	No	No

# Policy Evolution: Acceptable Use, Rules of Use

New Post | My View | MyLinks | People | Communities | IWE Library | Topics | IWE | Go

Go back to previous page | Add to Watch List | Like | Additional Options

Information | Table of Contents

Owner: Peter Dallaway (Offline)

Contributors

About | Help | Feedback | Preferences

## Mobility Policies and Eligibility

This page contains information and links relating to:

- Who is eligible for Cisco-paid mobility services.
- Cisco's **Mobile Voice and Mail Service (Personal Plan)**
- The Rules of Use for using

EMAN > Client Services > Mobile Phones

**Mobile Mail (Personal Plan)**

- NEW USER
  - Request Service
  - Setup Mobile Mail Service
- EXISTING USER
  - Corporate Conversion
  - Setup Mobile Mail Service
  - Change Service
  - Cancel Service
  - Check Status
  - Open a Case

### Mobile Voice and Mail (Personal Plan) > Setup Mobile Mail Service > Rules of Use

Please follow the link below to view the full "Rules of Use" information specific to the mobile service type you are requesting, then return here to tick the box and click "I Agree."

[Rules of Use](#)

- Cisco reserves the right to delete data from your Cisco-enabled mobile device, either directly or "over the air," if Cisco confidential information is deemed likely to be compromised. Further, it is likely that any personal data, third-party applications or operating system files stored on the device would be deleted in this process as well. You acknowledge and agree that Cisco shall bear no liability for loss or damage resulting from such action.
- All handheld devices storing Cisco Confidential Information require a minimum of a 4-digit PIN with a maximum 10-minute inactive timeout to secure access to the device.
- When a handheld device is lost or stolen, Internal Technical Support (GTRC) must be contacted immediately in order to properly disable corporate connectivity services, and if possible, remotely erase Cisco Confidential Information from the device.

☐ Please tick the box and click "I Agree" to confirm that you have read and accept the "Rules of Use" policy

The Rules below are designed to:

- Unnecessary cost.
- Non-compliance with applicable

Robot Wan edited David Chu's post CPE Milestone Date Action Items Today 11:11





# Hard Work & Results: Company Gains





# Hard Work & Results: Company Gains We Also Project:



# BYOD Application

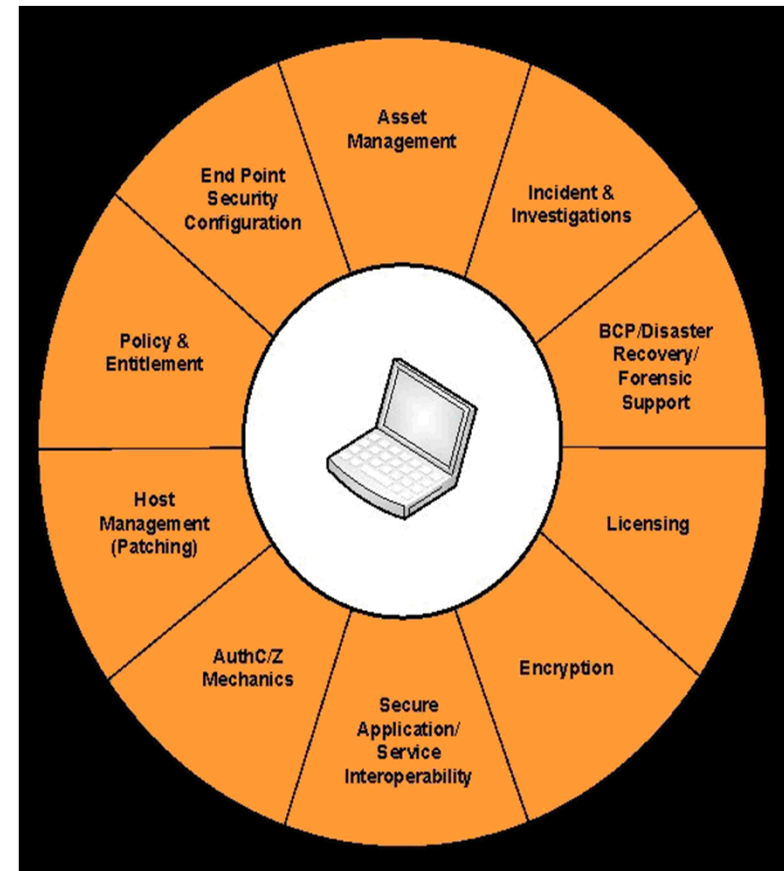


**RSA**CONFERENCE**2012**

# Top 10 - Major IT “BYOD” Questions

How To:

- Increase visibility and policy based control?
- Deal with Architectural Change?
- Enable Service Delivery?
- Manage Identity, Entitlement & Access?
- Maintain Cost, Licensing & Asset Controls?
- Manage Deperimeterization Scenarios?
- Understand Impact to Compliance?
- Maintain Standards?
- Deal with Application Interoperability?



# How to Embrace Mobility While Ensuring Security

## Some Questions to Answer

- Do I have the WLAN capacity and reliability to support increase in mobile devices and future applications?
- How do I enforce security policies on non-compliant devices?
- How do I grant different levels of access to protect my network?
- How do I ensure data loss prevention on devices where I don't have visibility?
- How do I minimize emerging threats targeted at mobile devices?
- How do I monitor and troubleshoot user and client connectivity issues on my access (wired/wireless) network?
- Is my network capable of delivering the scalability and performance required to realize the benefits of a BYOD strategy?





# Summary

On Your BYOD Journey



## Establish Governance

- Business Sponsors
- HR and Legal



## Align to Broader IT strategy

- Workforce Enablement & Mobility
- Globalization & New Business Model
- Cloud Transition



## Take a user Centric Approach

- Employees, Contractors, Partners
- Balance Risk Management with TCO, User Experience and Security



## Take Architectural & Phased Approach to Delivery

- Bake Security Architecture into the broader business and IT architecture
- Educate & Communicate



Thank You



**RSA**CONFERENCE**2012**