Information Security Decisions

TechTarget

Closing Keynote Address:

When Business Processes Fly the Coop

G. Mark Hardy, CISSP, CISM
President, National Security Corporation
gmhardy@nationalsecurity.com
+1.410.933.9333

Agenda

- Business processes
- Technology evolution
- BYOD impact
- Consequences
- Enterprise App Stores
- A “New Deal”
- The future

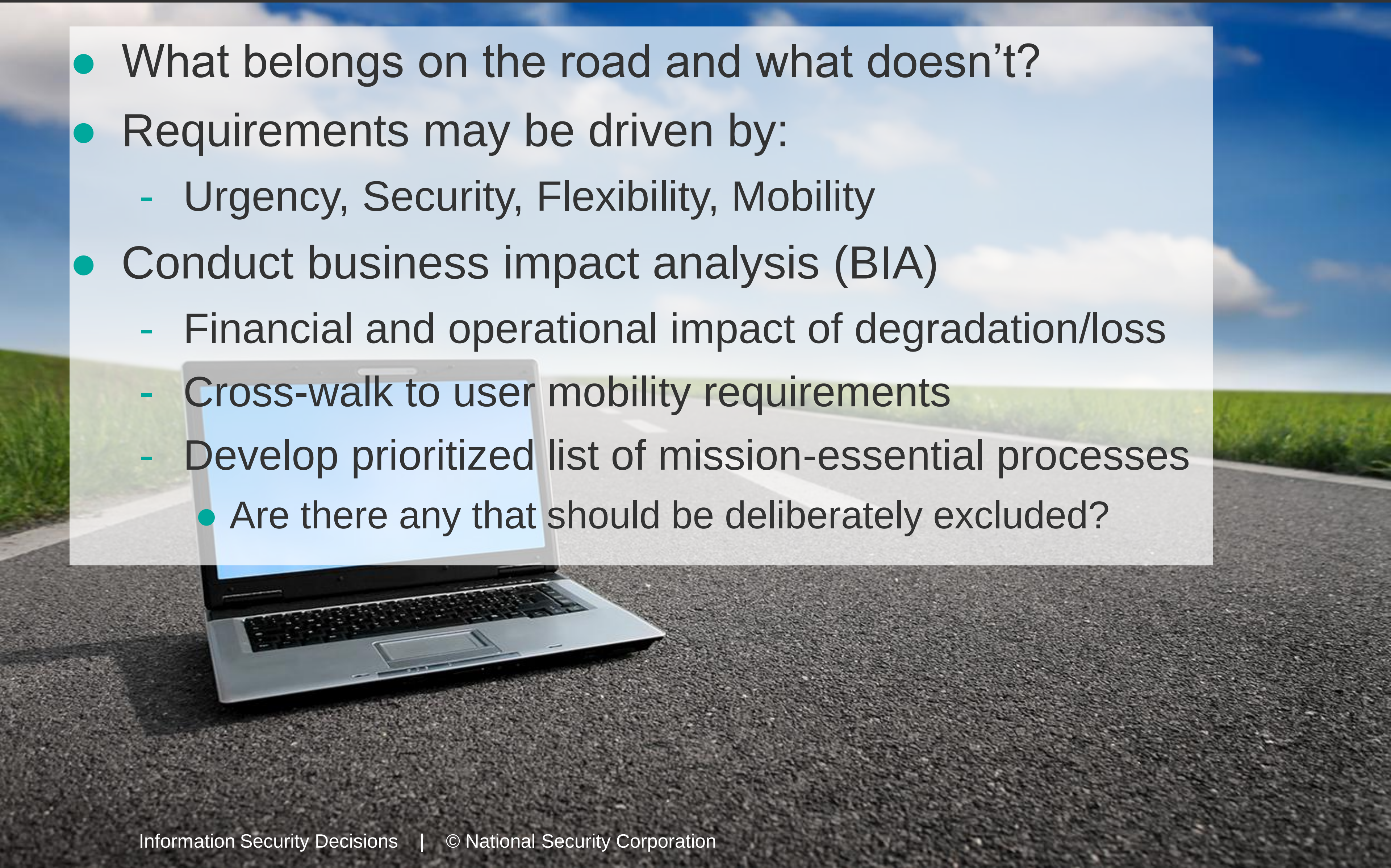
TechTarget

Business Processes

What Business Processes Do We Care About?

- Anything that can go on the road
  - These days, what can't?
- One school of thought: mission critical
  - E-mail
  - Corporate communications
  - Required for business (travel, expenses, ordering, etc.)
- Another school of thought:
  - The apps drive the problem, not the business processes
    - It's not what you're supposed to be doing, it's what you are doing

How Do We Determine Criticality?



- What belongs on the road and what doesn’t?
- Requirements may be driven by:
  - Urgency, Security, Flexibility, Mobility
- Conduct business impact analysis (BIA)
  - Financial and operational impact of degradation/loss
  - Cross-walk to user mobility requirements
  - Develop prioritized list of mission-essential processes
    - Are there any that should be deliberately excluded?

Intersect Future Requirements

- “Skate to where the puck is going to be” – Wayne Gretzky
- Dilemma:
  - Hardware has a depreciation schedule of 5 years
  - No one knows what the state of the art will be in 5 years
- In 2008:
  - The current version of Windows was VISTA
  - There were no Android phones
  - The dominant smartphone OS was Symbian
  - Windows Mobile outsold iOS
- So how are we supposed to know what the world will look like in 2018?

Ref: http://en.wikipedia.org/wiki/Mobile_operating_system

Technology Evolution

A Brief History of Remote Computing

- 3270 green screens
- PC (standalone)
- PC (dialup)
- “Luggables”
- Portables
- Laptops
- PDAs
- Smart Phones
- Tablets
- Wrist computing
- ???

Futurama character © FOX and its related entities. Fair use claimed under 17 U.S.C. 107

Where Are We Going?

- Systems are:
  - Faster
  - Smaller
  - Cheaper

- More susceptible to:
  - Compromise
  - Loss / theft
  - Misuse

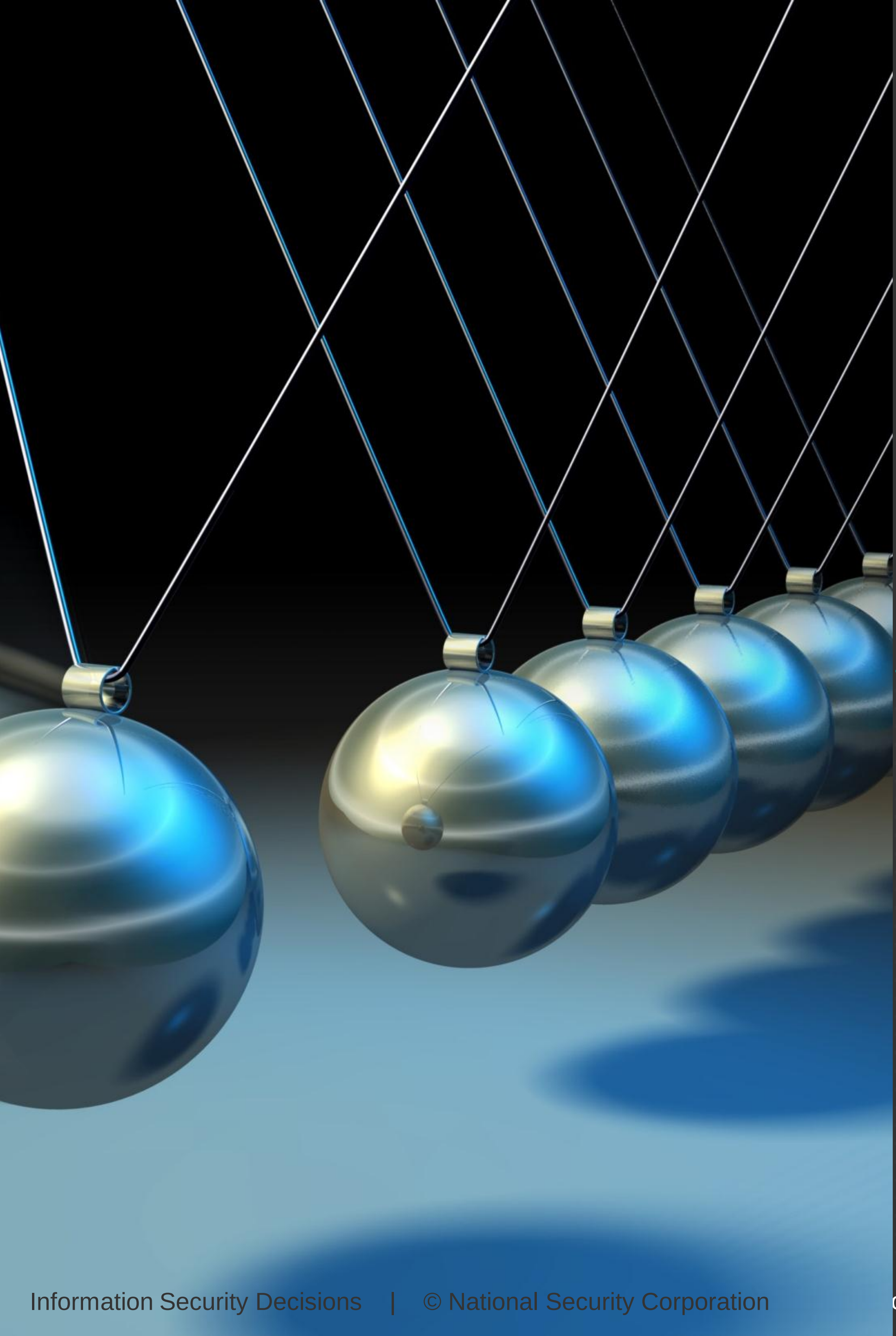
On balance, is this good or bad?

Bring Your Own Disaster

The Impact of BYOD

Why BYOD?

- First “killer app” was (is) e-mail
- Is your enterprise BYOD strategy requirements-driven or convenience-driven?
  - Do you even HAVE a strategy?
- Who is driving your BYOD?
  - Executives or workers? Why? Is this a good way to go?
  - How did you calculate your cost-benefit analysis?
- What does your risk analysis look like?
  - What’s on your SWOT analysis?
  - What are the compliance and regulatory implications?
  - Have you thought out the consequences, good and bad?



What Are The Consequences?

What Can Go Right?

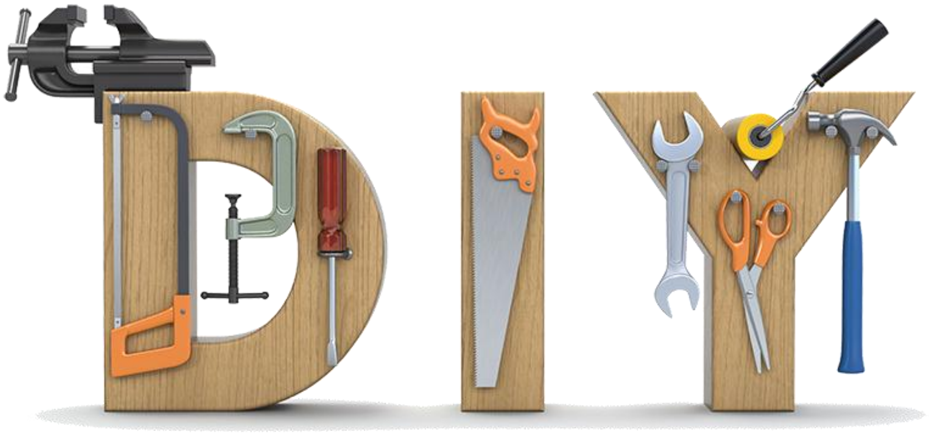
- We extend the capabilities of our workforce
  - Anytime, anywhere
- We can reduce decision cycles
  - More rapidly capture opportunities, respond to problems
- We enable collaboration
  - No requirement for physical proximity to work together
- Meets expectations of younger work force

- What else? (These can become your business case drivers)

What Can Go Wrong?

- Lack of control
  - Infrequent or no backup
    - How much unique content is being created on remote devices?
  - Data sharing
    - How do you do DLP or IDS outside your perimeter?
  - Maintaining updates
    - Can you “push” effectively, or do users have to “pull”?
- Data compromise
  - “Convenience is the enemy of security” – Bruce Schneier
  - How do you even know when or if you’ve lost it?
- Do the risks outweigh the benefits?
  - Does that even matter if your culture demands it?

DLP = Data Loss Prevention, IDS = Intrusion Detection System

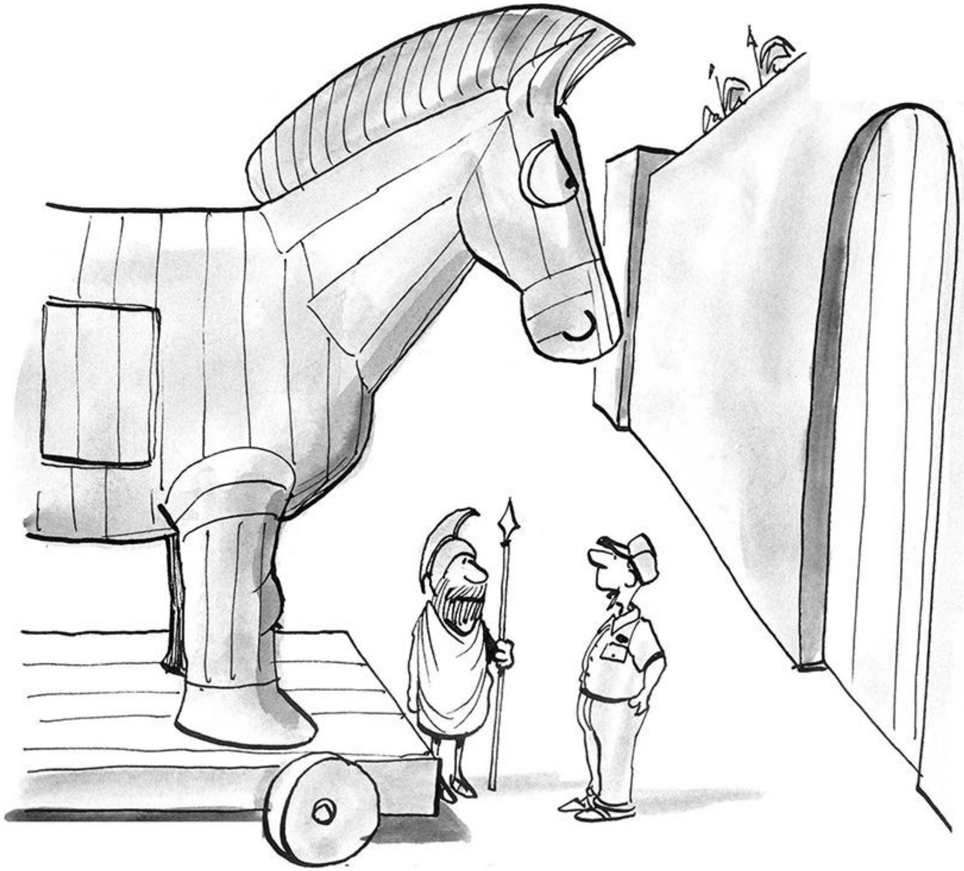


The Case for Rolling Your Own

What’s the Problem?

- Who provisions your equipment?
  - Do you have a locked-down configuration?
  - Can you detect jail-broken / rooted devices?
  - How do you know when new apps get added?
- Where do your users get their apps?
  - 79% of mobile malware targets Android[1]
  - 238 security problems specific to iOS devices in CVE database[2]
  - Georgia Tech students have demonstrated how to insert a malicious app into Apple’s App Store[3]
  - "96% of the top 100 paid mobile apps have been hacked"[4]

Ref: 1. http://abcnews.go.com/Technology/android-target-79-percent-mobile-malware-government-report/story?id=20096620
2. http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=iOS
3 https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_wang_2.pdf
4 http://www.computerweekly.com/news/2240161740/At-least-9-out-of-10-top-mobile-apps-hacked-study-shows



“Sure, bring her in. I’ve always wanted to work on one of these babies.”

The Open App Store model is broken

The Problem is a Complete Loss of Trust

What About Device Vendors Themselves?

- Samsung KNOX
  - Customizable Secure Boot
  - Continuous Linux kernel monitoring (can force shutdown if compromised)
  - Isolation of applications and data into secure container
- BlackBerry Balance
  - Separates work and personal apps and data
    - Cannot cut/paste from one domain to another
    - Allows wiping of work apps and data without wiping personal
- Apple iOs
  - Low-level hardware/firmware protection, strong encryption
    - (security glitch in iOS 7 notwithstanding)

Ref: http://www.samsung.com/global/business/mobile/solution/security/samsung-knox
http://us.blackberry.com/business/software/blackberry-balance.html
http://www.apple.com/iphone/business/it-center/

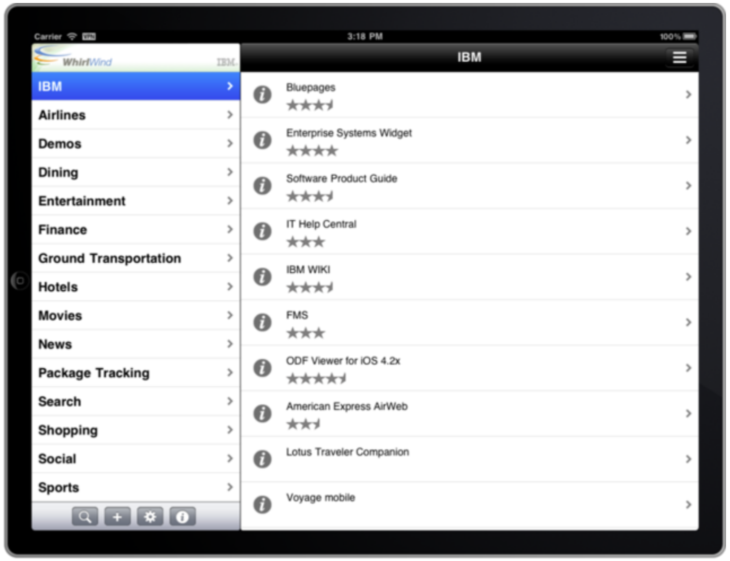
"'Garbage in, garbage out,' isn't exactly true. 'Garbage in, garbage stays … Then it gets pregnant and gives birth to triplets.'"

-- Nido Qubain

But That Isn't ENOUGH

What Do You Do If You Don’t Trust App Stores?

- "Self-provisioning is the long-term trend." [1]
  - IBM built own app store called WhirlWind
    - Concept started in 2009
    - In production by 2010
    - Supports Android, iOS, BB



- "Many providers [allow] you to simply upload and manage applications automatically" [2]
  - Vendors allow you to manage your own enterprise app store
  - "Provisioning profiles ... operate just like a regular mobile app store"

Ref: 1 Jon Brodkin, http://arstechnica.com/business/2011/11/private-app-stores-does-your-company-need-its-own/
2 Chris Moyer, http://searchcloudapplications.techtarget.com/answer/Build-an-in-house-enterprise-app-store-without-breaking-the-budget

Consider an Enterprise App Store (EAS)

We Need A "New Deal"

You Can Use iOS for Custom B2B Apps

- You:
  - Develop custom B2B app
  - Update iTunes Connect account
  - Select price and identify customers and release date
  - Submit for review
    - But be careful about sensitive data
- Customers:
  - Enroll in Volume Purchase Program for Business
  - Download apps
  - Distribute apps to users
- BUT … have to follow directions and synch with iTunes

Ref: https://developer.apple.com/programs/volume/b2b/

You Can Let Users Come To You

- Another alternative is to deploy your own webpage
  - Downloadable applications for mobile users
- But how do you:
  - Update users after they've downloaded an app?
  - Track software versions in the field?
  - Manage distributed apps?
- Also, how do you secure an "open" URL?
  - Just because it's not published doesn't mean someone else can't find it
  - Can you effectively do client-side authentication?

Ref: https://discussions.apple.com/thread/2670038?start=0&tstart=0, comments by "chuckfromboston"

(Fortunately, there are solutions)

This Sounds Like a Royal Pain in the EAS

How About Running Your Own Enterprise App Store (EAS)?

- According to Ian Finley of Gartner:
  - "By 2017, 25 percent of enterprises will have an Enterprise App Store"
  - "Bring your own application (BYOA) has become as important as bring your own device (BYOD)"
  - Key Enterprise App Store trends:
    - More mobile devices and use of MDM will drive enterprise app stores. (App stores should be part of a full MDM solution)
    - EAS can automate license procurement down to user level
    - EAS success depends on increased supply of software

Ref: Ian Finley, http://www.gartner.com/newsroom/id/2334015

Build Your Enterprise App Store Correctly

- Use platform-agnostic apps that work on anticipated devices
- Build a sufficiently large catalog of useful and desirable apps
- Ensure you have a workable subscription management schema
- Make the app store an experience, not an endurance
- Build it and field it SECURELY

Ref: Jay Manciocchi, "10 Steps for Building a Successful Enterprise App Store", http://saasmarkets.com/10-steps-for-building-a-successful-enterprise-app-store/

Benefits of Enterprise App Stores

- Anytime, anywhere access
- Can serve internal employees and external customers
- Improve security and control over app distribution and updates
- Reduce software management costs (maybe?)
- Increase customer engagement through sharing of key apps and data

Ref: Jay Manciocchi, "10 Steps for Building a Successful Enterprise App Store", http://saasmarkets.com/10-steps-for-building-a-successful-enterprise-app-store/

But …

- How do you ensure devices are not jailbroken or infected with malware?
  - Need to integrate with a Mobile Device Management (MDM) solution
  - You DO have one, right?
- Can you require users to use ONLY your private app store?
  - Are private web stores allowed to sell Apple apps? (probably not)
  - Is there an equivalent of a web app firewall to interdict what apps can be accessed from a public store? (probably)

How Do We Combine BYOD with EAS?

- BYODEAS doesn’t show up on Google search (yet)
- Can work with CYOD (choose your own device)
- How can we create a framework to enable security in BYOD?
  - Offer a partial financial subsidy toward monthly bill
  - Create a legal contract (must be an exchange of value)
  - Allows us to enforce security requirements
    - Remote wipe
    - Encryption
    - Key escrow
  - Manage access control (just keep the cat away from your iPhone 5)
- Or, just accept the risks

The Future

Where Do We Go From Here?

- We’re looking at a new model for a mobile ecosystem
- There are several vendors offering solution sets (these are examples, not endorsements):
  - SAP Afaria
  - Apperian
  - BMC Software's Partnerpedia
- But we have to solve the desirability/usability problem
  - Create awareness
  - Communicate availability and capabilities
  - Get users to appreciate advantages
    - Right applications, right version, securely

Ref: http://tech.fortune.cnn.com/2011/06/28/your-companys-own-app-store/

The Future

- Apps will need to support iOS and Android
  - Might be interesting if Windows (8) makes a comeback
- User convenience will compete with enterprise requirements
  - Security, usability, availability, remote control
- Expect open-source EAS frameworks
  - Maybe even a standard or two?
- Vendors will drive hardware/software convergence
  - Apple/iOS already there; Microsoft/Nokia and perhaps Samsung/Android
- Strong client authentication along with decryptable apps in the App Store might be a viable alternative to EAS
  - Need to solve the trust model with the store host

Thank you! Questions?

G. Mark Hardy, CISSP, CISM
President, National Security Corporation
gmhardy@nationalsecurity.com
+1.410.933.9333