Work/Life separation

Protecting enterprise data on user owned devices

Nicko van Someren

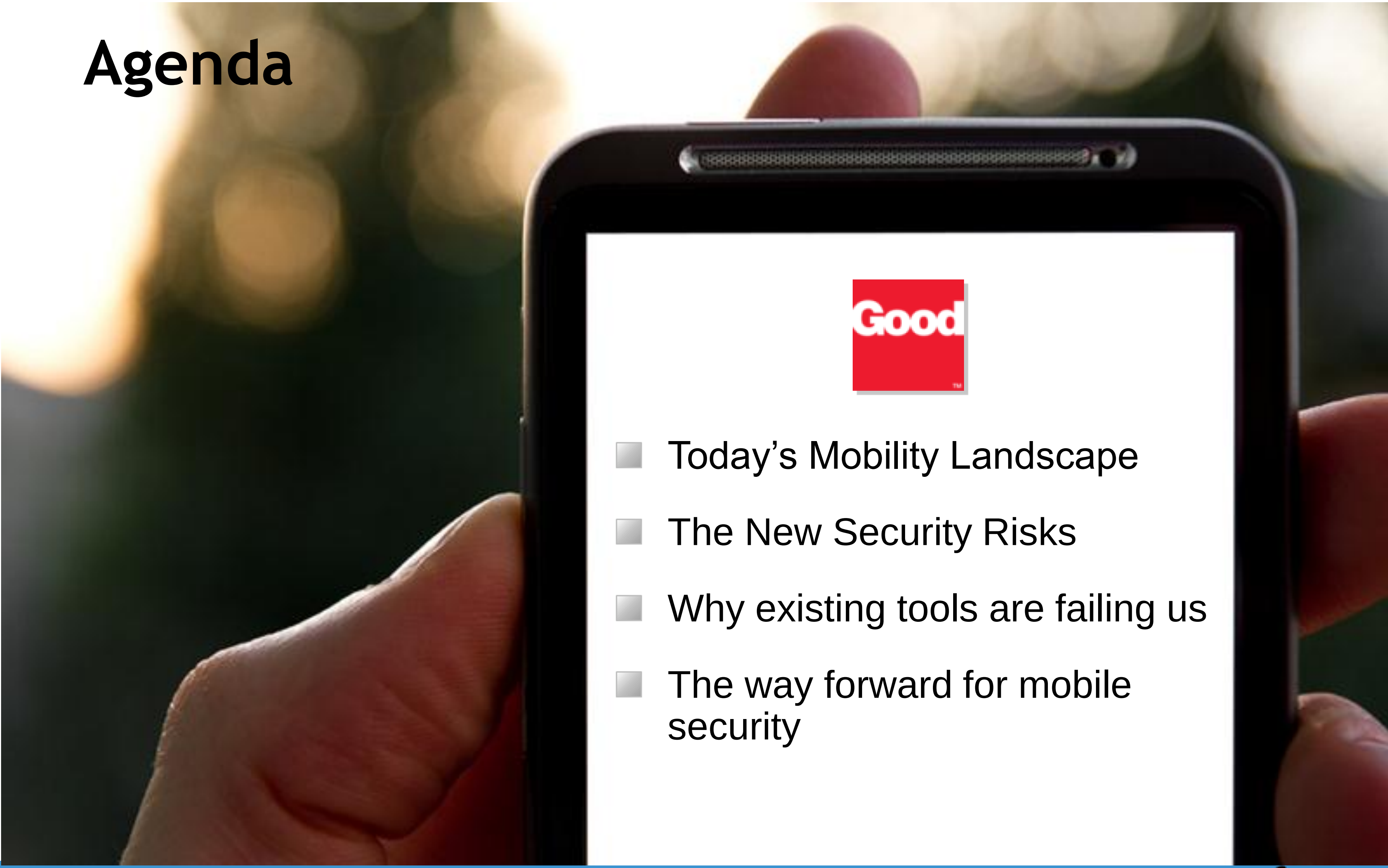
CTO, Good Technology Inc

Session ID: DAS-402

Session Classification: Intermediate

RSACONFERENCE2012

Agenda

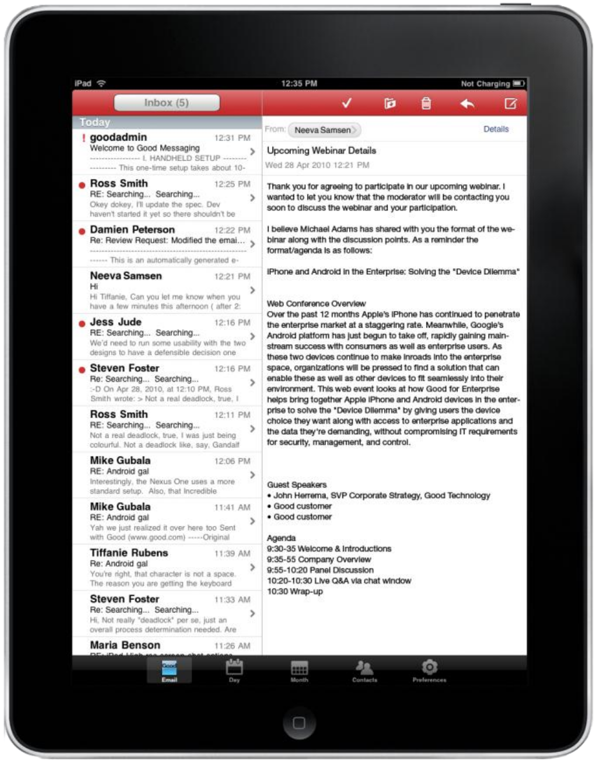


- Today’s Mobility Landscape
- The New Security Risks
- Why existing tools are failing us
- The way forward for mobile security

A Changing Mobility Landscape

From corporate-issued Blackberry devices

…**to proliferation of** non-Blackberry personal devices with easy access to a wide variety of apps



goodadmin 12:31 PM
Welcome to Good Messaging
---------------- I. HANDHELD SETUP --------
--------- This one-time setup takes about 10-

Ross Smith 12:25 PM
RE: Searching... Searching...
Okey dokey, I'll update the spec. Dev haven't started it yet so there shouldn't be

Damien Peterson 12:22 PM
Re: Review Request: Modified the emai...
------ This is an automatically generated e-

Neeva Samsen 12:21 PM
Hi
Hi Tiffanie, Can you let me know when you have a few minutes this afternoon (after 2:

Jess Jude 12:16 PM
RE: Searching... Searching...
We'd need to run some usability with the two designs to have a defensible decision one

Steven Foster 12:16 PM
Re: Searching... Searching...
:-D On Apr 28, 2010, at 12:10 PM, Ross Smith wrote: > Not a real deadlock, true, I

Ross Smith 12:11 PM
RE: Searching... Searching...
Not a real deadlock, true, I was just being colourful. Not a deadlock like, say, Gandalf

Mike Gubala 12:06 PM
RE: Android gal
Interestingly, the Nexus One uses a more standard setup. Also, that Incredible

Mike Gubala 11:41 AM
RE: Android gal
Yah we just realized it over here too Sent with Good (www.good.com) -----Original

Tiffanie Rubens 11:39 AM
Re: Android gal
You're right, that character is not a space. The reason you are getting the keyboard

Steven Foster 11:33 AM
Re: Searching... Searching...
Hi, Not really "deadlock" per se, just an overall process determination needed. Are

Maria Benson 11:26 AM

From: Neeva Samsen Details

Upcoming Webinar Details
Wed 28 Apr 2010 12:21 PM

Thank you for agreeing to participate in our upcoming webinar. I wanted to let you know that the moderator will be contacting you soon to discuss the webinar and your participation.

I believe Michael Adams has shared with you the format of the webinar along with the discussion points. As a reminder the format/agenda is as follows:

iPhone and Android in the Enterprise: Solving the "Device Dilemma"

Web Conference Overview
Over the past 12 months Apple's iPhone has continued to penetrate the enterprise market at a staggering rate. Meanwhile, Google's Android platform has just begun to take off, rapidly gaining mainstream success with consumers as well as enterprise users. As these two devices continue to make inroads into the enterprise space, organizations will be pressed to find a solution that can enable these as well as other devices to fit seamlessly into their environment. This web event looks at how Good for Enterprise helps bring together Apple iPhone and Android devices in the enterprise to solve the "Device Dilemma" by giving users the device choice they want along with access to enterprise applications and the data they're demanding, without compromising IT requirements for security, management, and control.

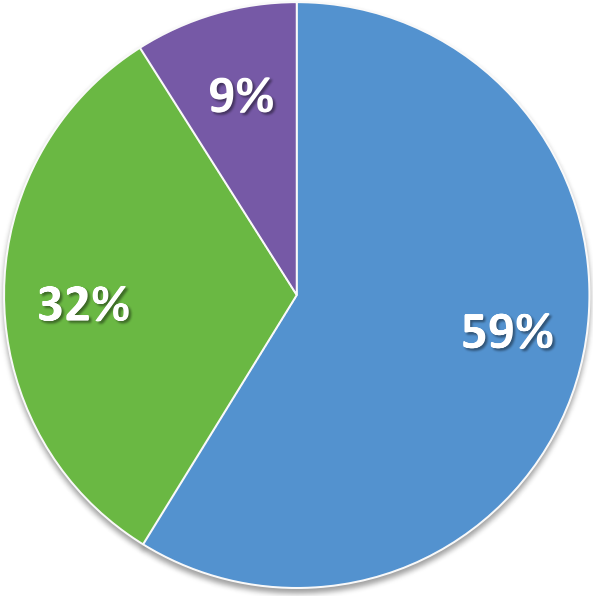
Guest Speakers
- John Herrema, SVP Corporate Strategy, Good Technology
- Good customer
- Good customer

Agenda
9:30-35 Welcome & Introductions
9:35-55 Company Overview
9:55-10:20 Panel Discussion
10:20-10:30 Live Q&A via chat window
10:30 Wrap-up

Access to work data on personal devices

- Users **really** want to access their work data on their own mobile devices
  - They don’t want two devices
  - Blackberries just aren’t cool!
- You can’t stop it happening
  - So embrace it before it’s too late
- If you work out how to do it then you can save money
  - Save CapEx by not buying the devices
  - Save OpEx by not paying for the data plans

"Bring-Your-Own-Device"
It's Already Here and Will Continue to Grow



Survey Question: Do you plan to support BYOD?

- 🟦 Already Support
- 🟩 Planning to Support
- 🟪 No Plans to Support

- January 2011 survey to Good customers
  - 400+ respondents from variety of industries
  - Financial Services, Healthcare, Government, Legal & other Professional Services, Technology, & Manufacturing
- Nearly 59% already support BYOD model – another 32% plan to do so
- Financial Services accounted for the most responses, over 30%
- Financial Services showed most existing support for BYOD – 57% overall and 67% for firms with 3K+ employees

Source: Good Technology customer survey 2011

New Technology Creates New Challenges

> *Easy mobility combined with powerful consumer devices significantly increases the **risk of unplanned exposure of company information**.*

Gartner

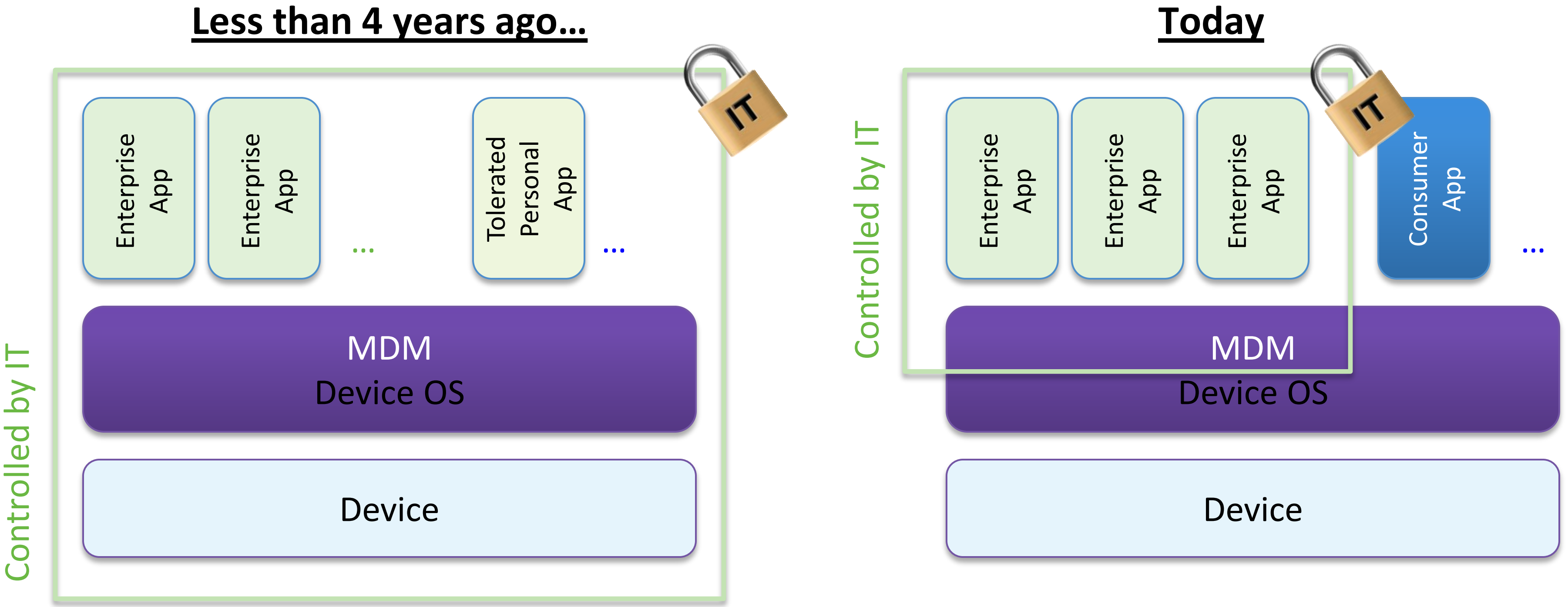
Four Architectural Approaches to Limit Business Risk on Consumer Smartphones and Tablets

– Dec 2010, John Girard, Ken Dulaney

- Government and Enterprises IT organizations are grappling with
  - How do I secure non-Blackberry devices?
  - How do I minimize data loss on consumer mobile devices?
  - How do I support personally-owned and corporate issued devices cost-effectively?
  - How do I manage personally-owned devices while respecting employee privacy?

Why is Risk Increasing?

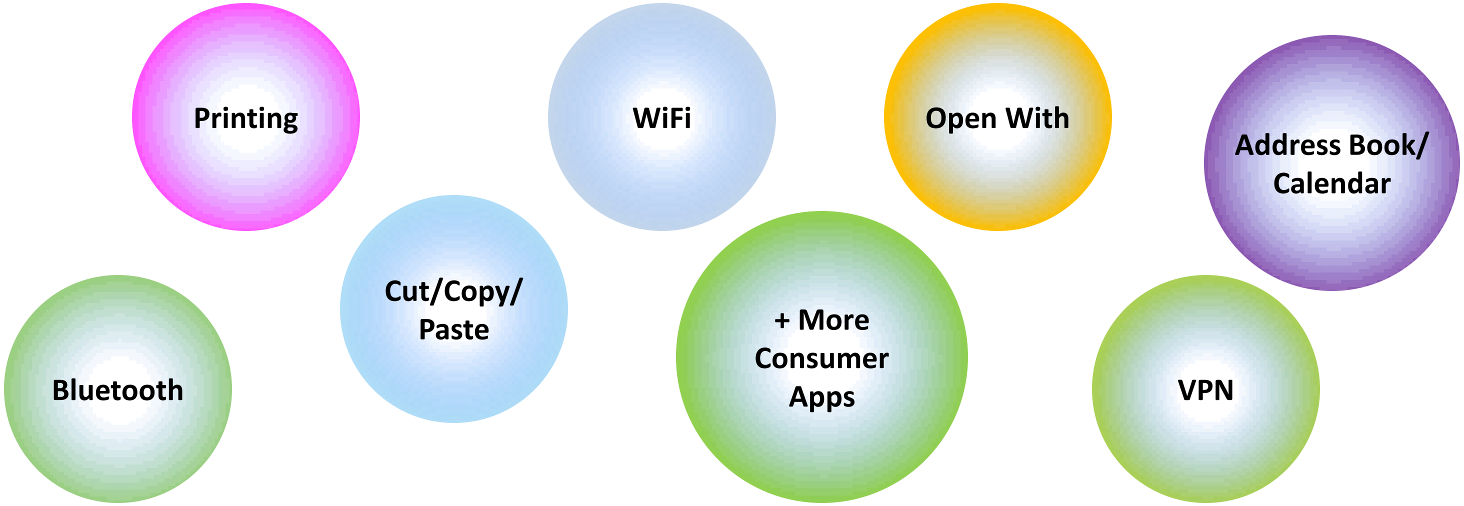
- Securing Mobile Devices is re-defined



On-device data encryption and secure back-end connectivity remain essential… but are not enough anymore to prevent data loss…

Myriad Opportunities for Data Loss

Modern mobile OSes offer a whole host of ways for data to leave your control



Printing

WiFi

Open With

Address Book/ Calendar

Cut/Copy/ Paste

+ More Consumer Apps

Bluetooth

VPN

Once activated, services offered at the OS level are available to both Enterprise and Personal Apps!

The OS vendors go out of their way to make it easy for Consumer and "Prosumer" apps to consume data exposed by native and enterprise apps

As a Result…

This fundamental change significantly increases the Risk of Data Loss. This risk is exacerbated by a loss of control over consumer app availability.

- VPN Scenario
  - Opening VPN provides OS level access to corporate intranet
  - Any app store/marketplace browser can be used, including ones that integrate a ‘drop box’
  - Company docs can thus be downloaded in a non-secure app

- Attachment “Open with”
  - Email client provides the ability to “open with” attachment using any app store/marketplace app designed and registered to manipulate documents
  - Once in the non-secured app, documents can be potentially leaked anywhere

MDM Solutions to the Rescue?

By nature, pure MDM solutions are not enough to prevent data loss.

No pure MDM Solution can prevent the risk of data loss for the two previous scenario – unless App Store / Marketplace are turned off.

Blacklisting doesn’t work either – not supported by all platforms and, even if it was, no realistic way to maintain when thousands of new apps are developed every day.

Security Starts at the Application Level

> *Managing these devices will help, but companies should also consider the roles of other technologies and application practices that reduce data exposure and leakage.*
>
> Gartner
>
> Four Architectural Approaches to Limit Business Risk on Consumer Smartphones and Tablets – Dec 2010, John Girard, Ken Dulaney

Gartner’s Implementation Advice

- “Give preference to self-securing applications from independent software vendors (ISVs) and internal development groups”
- “Do not assume that device management policies will protect business interests and access controls…”

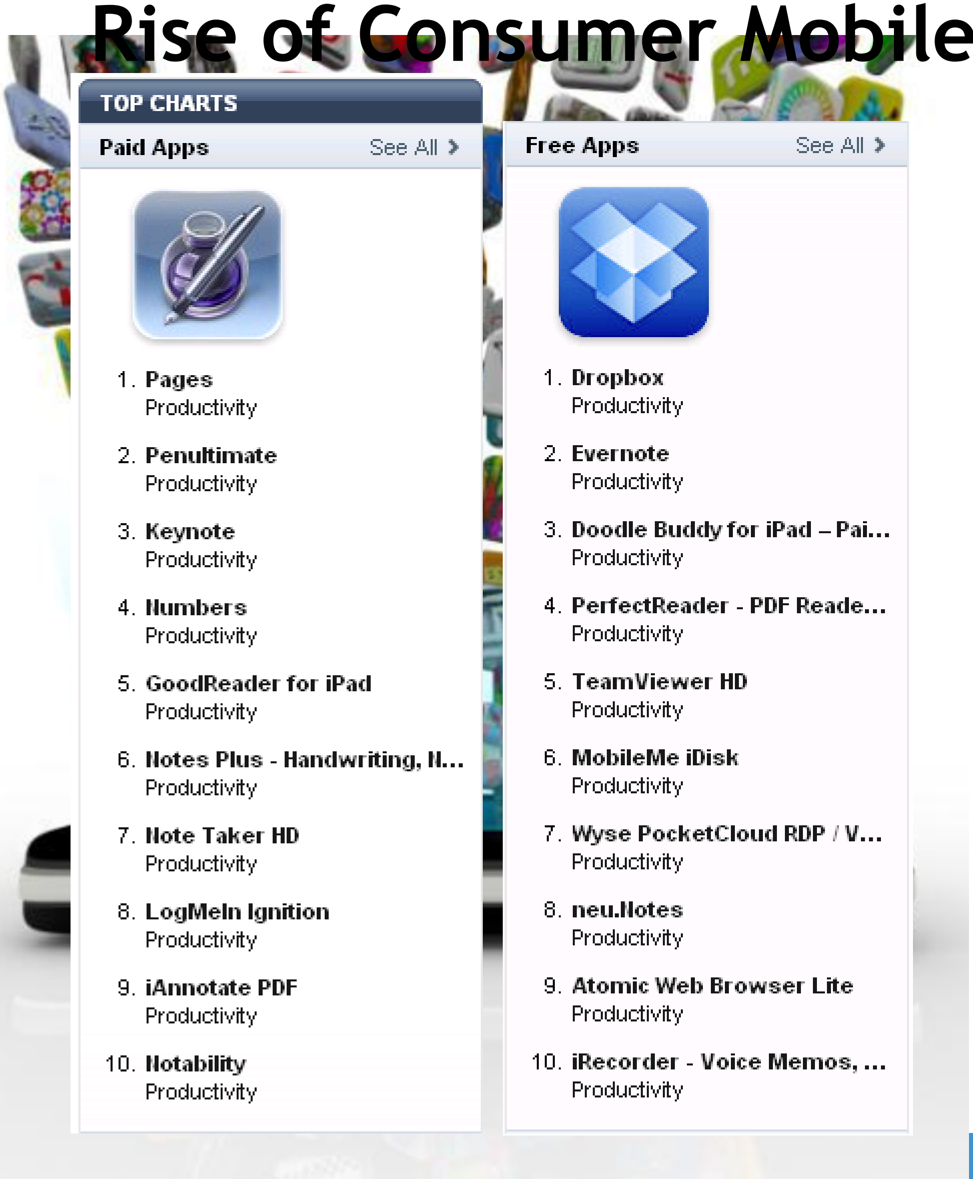
Source: Four Possible Architectural Approaches to Limit Business Risk on Consumer Smartphones and Tablets, G00208145, Gartner, Dec 2010

The New Security Risk: The Well Intentioned User

What do they have in common?

- Tech savvy
- Access to powerful computing tools
- Will do whatever it takes to get the job done
- Will try to find a way around IT security measures

Rise of Consumer Mobile Apps Increases Risk



TOP CHARTS

Paid Apps See All ›

1. Pages
   Productivity
2. Penultimate
   Productivity
3. Keynote
   Productivity
4. Numbers
   Productivity
5. GoodReader for iPad
   Productivity
6. Notes Plus - Handwriting, N...
   Productivity
7. Note Taker HD
   Productivity
8. LogMeIn Ignition
   Productivity
9. iAnnotate PDF
   Productivity
10. Notability
    Productivity

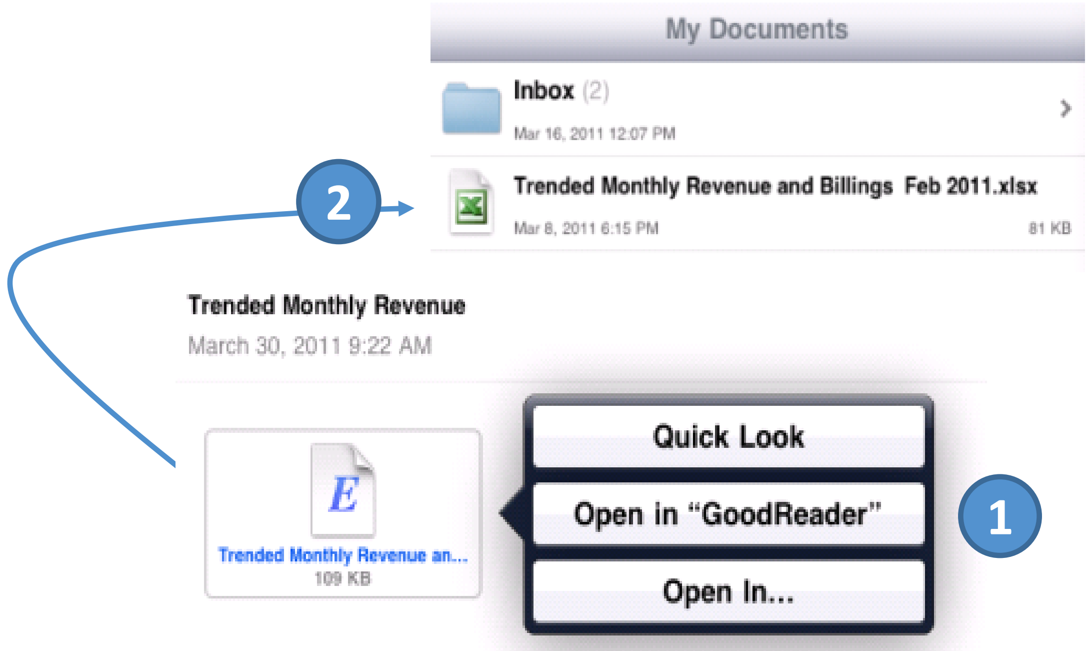
Free Apps See All ›

1. Dropbox
   Productivity
2. Evernote
   Productivity
3. Doodle Buddy for iPad – Pai...
   Productivity
4. PerfectReader - PDF Reade...
   Productivity
5. TeamViewer HD
   Productivity
6. MobileMe iDisk
   Productivity
7. Wyse PocketCloud RDP / V...
   Productivity
8. neu.Notes
   Productivity
9. Atomic Web Browser Lite
   Productivity
10. iRecorder - Voice Memos, ...
    Productivity

Source: Apple AppStore

- "There's an app for that"
- Most popular business apps
  - Document Handling
  - Annotation/Notes/Memos
  - Remote Desktop/Apps
  - Remote Printing
  - Web Conferencing
- Increases productivity, but also increases risk

Data Loss in 3 Easy Steps

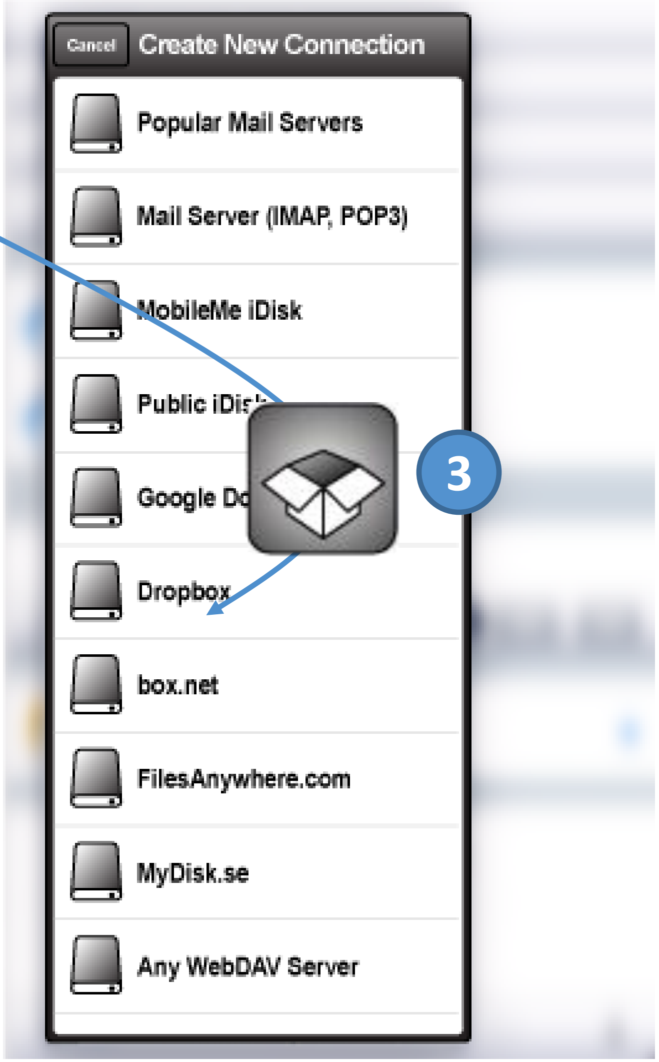

My Documents

Inbox (2)
Mar 16, 2011 12:07 PM

Trended Monthly Revenue and Billings Feb 2011.xlsx
Mar 8, 2011 6:15 PM
81 KB

Trended Monthly Revenue
March 30, 2011 9:22 AM

Trended Monthly Revenue an...
109 KB



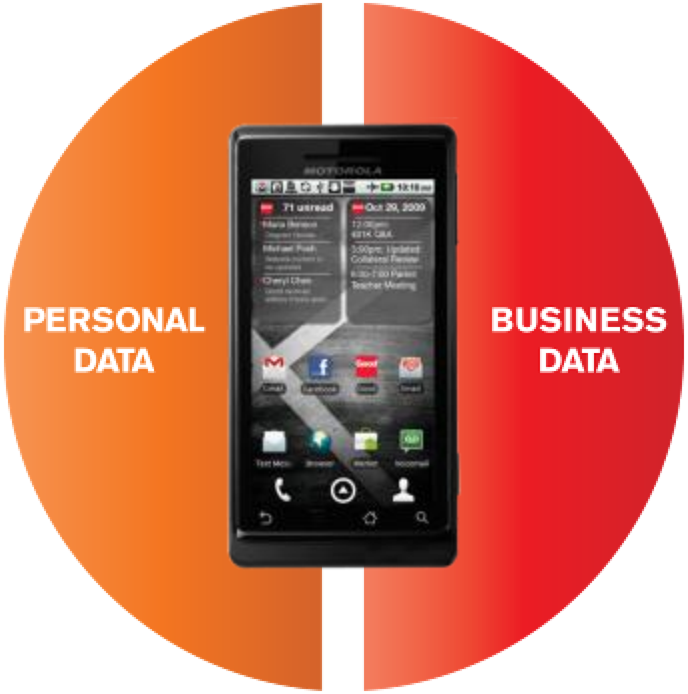
This might happen …

This is already happening!

What’s the Best Answer?

- Separate “personal” from “work” data
- Implement security, data loss prevention and management at the *application level* for all apps that need to see sensitive data
- Apply consistently across multiple mobile platforms – even where underlying platform doesn’t support

Secure Container



Separate Personal and Enterprise Data

Personal Data

Devices remain personal, untouched by enterprise

- Justifies shared employee expense

Freely access your applications

- Music
- Pictures
- Videos

Enterprise Data

Enterprise data lockdown

- Data encryption
- Password policies
- Remote wipe
- Secure data at rest

Access corporate apps

- Email, attachments & PIM
- Intranets
- Collaboration tools (e.g. Sharepoint)
- Web-enabled applications

Employees are more likely to accept an “enterprise-grade” mobile security policy when enterprise control is “contained” and does not impact personal experience, apps, or data

The Power of the App Store™

- Simply locking your data into a single container is not enough
  - The power of modern mobile OSs comes from having a collection of small applications (Apps) that work together
  - Having a single, ridged sandbox around a single set of business functions means we fail to leverage this model
- To allow employees to make the most of their mobile devices for business we need to allow ***authorized*** apps to share information in a ***secure*** and ***controlled*** manner
  - We need to be able to enforce a single policy across a collection of apps, whether they come from ISVs or are developed in house

Controlling the Flow of Data

- Once enterprise data reaches a container that container must enforce a policy regarding how that data can leave again
  - This policy needs to be set by the enterprise, not the app vendor
  - Policies need to be consistent across all of the deployed enterprise apps
- Fine grain control lets users make the most of their data while keeping it protected
  - It must be possible to control data transfers by content type, on a per-app basis

HOWTO: Secure mobile enterprise data

- “Bring Your Own Device” is here, now, and it’s here to stay.
  - Get over it. ***Embrace*** it and the benefits it brings.
- Managing end users’ own devices is *not* the answer
  - ***Apply*** tools that manage the *data* rather than just the *device*
  - ***Ensure*** sure that any device management solution for BYOD complies with privacy laws
- Mobile platforms are deliberately designed to make information sharing easy
  - ***Implement*** appropriate controls over enterprise data that *enable* data sharing between containerized applications without allowing data to leak beyond your control

Thank you

Dr. Nicko van Someren
nicko@good.com

Session ID: DAS-402

Session Classification: Intermediate