Challenges of Mobile Computing –
Risks & Challenges of the on-the-go Workforce

ARMA Spring Seminar April 23 & 24, 2013

Penny J Quirk, ERM^M
Director, EIM Practice

William Perry, CRM
North American Information Manager
Managing information at the speed of business calls for extended security, and being able to apply RIM principles to devices not owned by the organization, cloud storage, drop boxes, and web mail. Today's employees expect to have unfettered access, causing a need to establish an effective manner to facilitate mobile computing devices. Knowing legal requirements and legal opinion on the management of information through the various tools and technologies is becoming an overwhelming challenge.

What are the guidelines that employees must adhere to in order to use their own devices within the organization's infrastructure.

This session addresses a comprehensive approach to mobile computing, to include risk factors, legal considerations, policies and tools.

Attendees will be encouraged to engage in discussions on how best to control information in the mobile computing environment.
• Internet traffic has grown exponentially since 60’s; reaching a Zettabyte by 2016

• Mobile devices are more powerful than supercomputers of 20 years ago

• May 2011 the UN declared the internet is a fundamental human right
• 1 out of 4 couples meet on the internet
• 2.5 devices per user
  • iPad, smartphone, digital reader, etc.

• 2/3rd of all data collected will be video by 2015
• Internet connection devices
  • 1000 in 1984 (primarily at work)
  • 1,000,000 in 1992
  • 1,000,000,000 in 2008
  • 12,500,000,000 in 2010
  • projected 50,000,000,000 in 2020

• More digital data was collected in 2012 than all the previous 5,000 years previous

• We currently live in a world that was barely imaged 20 years ago
• More than 70% of all US businesses support some level of BYOD
  • 80% have 2,000 employees
  • 60% have 5,000 employees
  • 35% have 10,000 employees
• 50% require employee purchase
• 45% are stipend or expense back
Does this apply to me?

Business Demands

• Mobile workforce
• Competitive edge
• Legitimate need

Corporate Culture

• Old school generation X, Y
• Avoiding constraints
• Perceived need
Finding Balance

GUIDANCE & ACCOMMODATIONS

Policies & Restrictions
Balancing Elements

• Mindful of culture

• Mindful of the environment

• Mindful of accomplishments

• Phased approach
One Policy

Single set of policies to address:

- What people can do on their devices
- What access rights to the network
- What applications can they access
Privacy Concerns

• Personal vs. Corporate Data

• Privacy Laws
  • EU
  • Canada
  • US
Mobile Device Management (MDM)

- What is the risks at the infrastructure level?
  - Do you need to know how and who is trying to access the enterprise?
- What rules are needed?
- How can those rules be enforced?
- Who is exempt from the rules?
- How granular must we be?
MDM Rules & Enforcement

• Use of approved apps
• Password requirements
• Privacy settings
• Certificate management
• WiFi

• Geo-fencing
• Wipe – complete or select
• Location
• Lost recovery
• Secure web browsing
MDM Rules & Enforcement

• Lock down of select applications in connection with location (geo-fencing)

• Shut-down of device when not in compliance

• Wiping of corporate data – lost, employment release

• Containerization – complete separation of corporate data into one application.  FIPS 140-2 compliant
Enforcement Alerts

• Alert Admin

• Alert Admin + User

• Block — block user from getting new corporate data

• Selective Wipe — wipe corporate data and pull device off network (this action is revocable). Personal data is left untouched.

• Full Wipe — wipe back to factory default (not revocable)
Closing

• Identifying and understanding need

• Understanding solution set
  • Solution
  • Technology

• Risk and Benefits
Thank you

Penny J Quirk, ERM
Director, EIM Practice
Penny.Quirk@Robbinsgioia.com
703.342.2438

William Perry, CRM
North American Information Manager
bilp@statoil.com
713.897.9987