BYOD…
The Challenges of Implementing a "Bring Your Own Device" Policy

MARK HARRIS, Ph.D.
KAREN PATTEN, Ph.D.

UNIVERSITY OF SOUTH CAROLINA

SC-GMIS

NETWORK & TELECOM WORKSHOP

SALUDA SHOALS RIVER CENTER

OCTOBER 18, 2012

Research Motivation

- *Business Mobility Technologies* – Cellular, wireless access to Internet, tablets, etc., are changing the way people work.
- Today, evolving Business Mobility –
  - Enabled by smart phones and connected devices
  - Raises new security concerns for all enterprises.
- This presentation
  - Discusses new Business Mobility security risks
  - Provides expert recommendations to reduce the risk
  - Reports on preliminary research into impacts of the risks

Overview

- The growth of Business Mobility smartphones and connected devices
- New Business Mobility security concerns
- Professional recommendations
- Examples from earlier Business Mobility technologies research
  - Small & Medium-sized Enterprises (SMEs)
  - College Students
- On-going research

Business Mobility I

"*Business Mobility gives employees the freedom to collaborate and transact business outside traditional workplaces and times.*" (Nokia, 2006, p. 2)

- New, evolving Business Mobility strategies leverage employee flexibility and productivity to improve customer services
  - Mobile phones include 'smartphones / feature phones'
  - Connected devices include 'tablets, PDAs, gaming consoles, and eReaders.

Business Mobility II

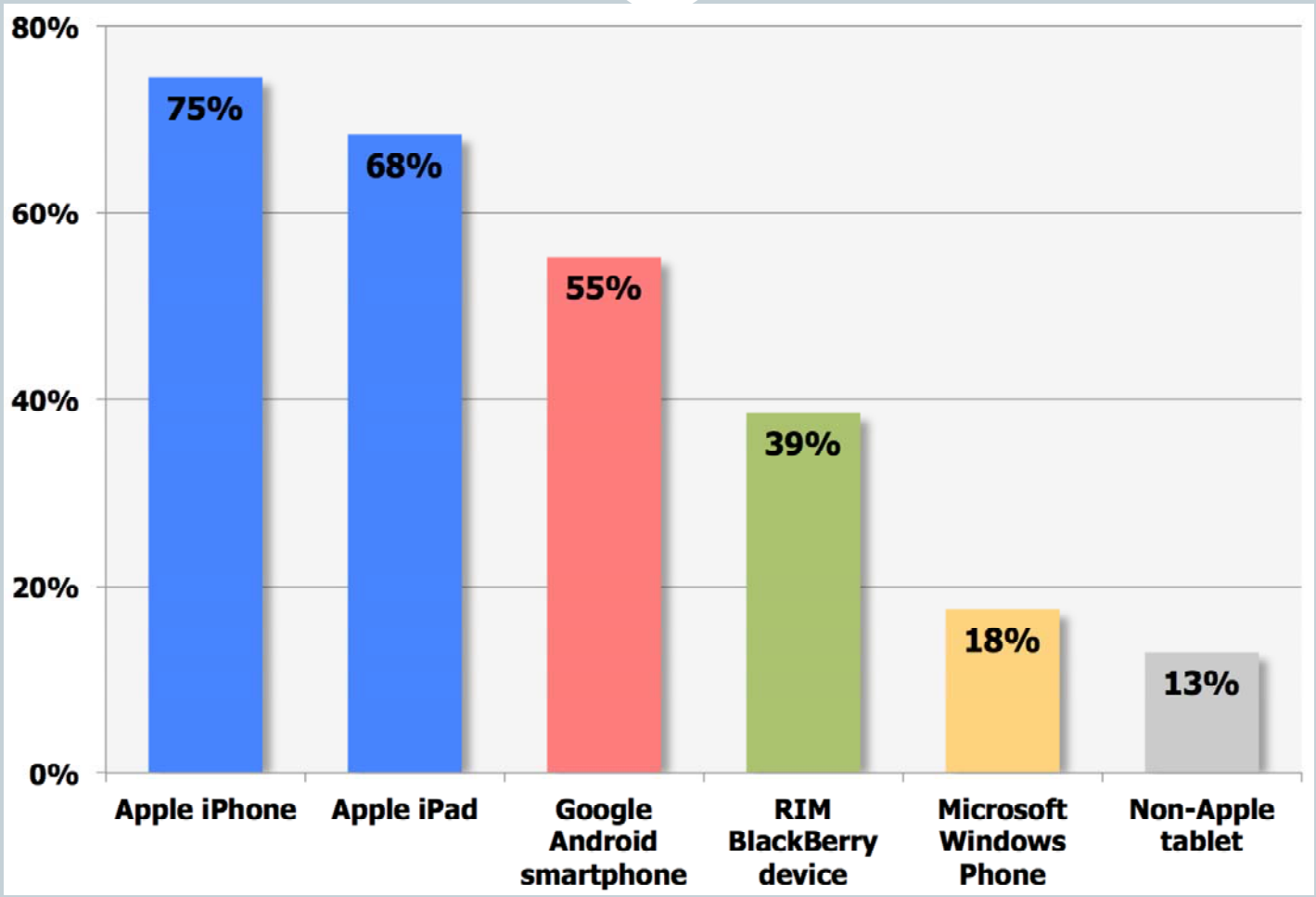
- However, these same Business Mobility strategies require *new policies* for addressing people, processes, and technologies
  - Mish mash of employee-owned and personal devices (BYOD)
  - Lack of systematic access to enterprise information
  - New security concerns

Mobile Device Statistics

(Osterman, 2012)

- By 2013, 50% of the workforce in medium to large businesses will use smartphones in the workplace
- 25% will use tablets in the workforce by 2013
- BYOD will cut corporate costs in the short run, but will add to them significantly if organizations do not deploy robust MDM capabilities
- By 2013, 50% of the workforce in medium to large enterprises will employ smartphones

Mobile User Demand



Mobile Threats

- Application-Based Threats:
  - Malware: malicious software
  - Spyware: collects user data without user's knowledge
  - Privacy Threats: apps that gather more personal information than necessary (e.g., location and contact lists)
  - Vulnerable Applications: contain software vulnerabilities that can be exploited.
- Web-Based Threats:
  - Phishing Scams: trick the user into providing information
  - Drive-by Downloads: automatic downloads on Web pages
  - Browser Exploits: exploits vulnerable browsers or launches software
- Network Threats:
  - Network Exploits: exploits flaws in the OS or other software that operates on local (e.g., Bluetooth, WiFi) or cellular (e.g., SMS, MMS) networks
  - WiFi Sniffing: intercepting WiFi communications
- Physical Threats:
  - Lost or Stolen Devices: access to personal information

New Mobile Malware

- Infects both browsers in iOS and Android
- Unsuspecting users get the malware by clicking on a link in a text message from what looks like their phone carrier.
- The malware can then track and record voice calls, text messages, emails, and can even track the phone's location.
- According to the security experts involved with this malware, there is *no known security software* that can detect this malware. (Dilanian,2012)

Wi-Fi

- As of mid-2011, 37.2 percent of U.S. digital mobile traffic and nearly 90% of tablet traffic occurred via a *WiFi connection* (Comscore, 2011).
- Cracking WEP now takes only seconds (Gold, 2011a).
- WPA was developed to fix the vulnerabilities of WEP and is also now easily cracked (Bradbury, 2011).
- WPA2 improved upon WPA
- With WPA2, most security experts were comfortable with its protection and many believed it was uncrackable (Gold, 2011a).
- September 2010, Elcomsoft's *Wireless Security Auditor* (WSA) was released, which could crack WPA2 passphrases.
  - The company's WSA software has the ability to brute force crack as many as 103,000 WPA2 passwords per second. The WSA software can also crack WPA.

Cellular Networks

- Cellular networks are not completely safe either.
- In 2010, Vodafone's cellular network in Europe was hacked through a device known as a femtocell (Gold, 2011b).
  - A femtocell is a miniature cellular base designed for localized use by homes and small businesses.
- The hacking can access victim's cell phones voice and data transmissions.
- Other companies, such as AT&T, Sprint, and Verizon, have since launched their own femtocells.

Apple iOS

- Runs third-party apps in an isolated environment.
- Prohibits all third party apps from reading/writing data outside of its own directory, which includes system files, resources, and the kernel.
- All third-party apps are granted access to the same data and capabilities.
- If a developer wants to access protected resources, they have to use registered Application Program Interfaces (APIs), approved by Apple.

Android

- Biggest target of mobile malware writers, with hundreds of malware programs detected (McAfee, 2011).
- An apps' capabilities are gated by "permissions" that the app declares upon installation
  - relies on end users' ability to evaluate permissions.
- Android apps are written in Java and run in a custom virtual machine, also providing process and file system isolation (Barrera & Oorschot, 2011).
- By default, apps only have read/write access to their own files, but the virtual machine itself has security flaws (Barrera & Oorschot, 2011).
- Developers can invoke libraries written in C/C++ which can run beyond the virtual machine boundaries (Barrera & Oorschot, 2011).
- This is different from Apple's iOS, where developers must use approved APIs to ensure security.

iOS Markets

- iOS
  - Limits user downloads to *official channels* (i.e., Apple's App Store)
  - The *curated model*:
    - consists of a certifying and vetting process before software is published, but this approach slows the process to market (Holbrook, 2011).

Android Markets – Open Distribution Model

- Users download from various sources (e.g. , Android Market, Amazon's Appstore for Android, Verizon V-CAST).
- Amazon's Appstore for Android and Verizon's V-CAST use a *curated model.*
- The Android Market uses a *community enforced model.*
- Google pulled numerous fake banking apps from the Android Market (Gunn, 2011)
- Android malware created a fake Android Market (Greenberg, 2011).
  - *Anything downloaded infected the device.*
- Google scans new applications in the Android Market for known malware and tests new applications in a simulated environment (Greenberg, 2012).
  - Google still doesn't screen developers like Apple does.
  - Google still allows applications to download and execute new code after installation, which bypasses the application screening process (Greenberg, 2012).

Example: Innovative SME IT Advantages

- Structure – SMES are not constrained by inflexible and legacy IT infrastructures
- Size – Organizational size and flexibility have fewer implementation issues
- Processes – SME processes are usually fluid and adaptable to new situations.
- Workplace – Dynamic workforces and workplaces require latest mobility capabilities and tools

(Patten & Passerini, 2007).

In-house Lower Cost Recommendations Minimum Security

1. Use *20+ character passphrases* with WPA2 if Wi-Fi is necessary
2. Install *antivirus software* on all mobile and connected devices (primarily Android)
3. *Password-protect* all mobile and connected devices
4. Have the capability *to erase data* on lost or stolen devices
5. Purchase *iOS products* over Android devices
6. *Sync* Apple products *with iTunes* on a regular basis (older versions)
7. Turn-off *discoverable Bluetooth*
8. *Update* the devices operating system and software *frequently*
9. Avoid storing usernames and passwords on the device or in the browser
10. Use *personal VPNs* (most are SSL, the weakest protection)
    1. Encrypt data from host to VPN Server, which is elsewhere
11. *Educate employees*!!!

In-house Higher Cost Recommendations More Secure

- Radius servers:
  - Provides better Wi-Fi network security than using a 20+ character pre-shared key.
  - Even Radius server authentication is vulnerable to *evil twin att*acks if the end user fails to properly identify the proper radius server (Nussel, 2010).
- Host a IPsec VPN internally
  - Protects data from the mobile device to the corporate network.
- Utilize *deep packet sniffing* on VPN packets
  - More secure than *stateful packet inspection*
- Use *two-factor authentication* for laptop and tablet remote access
  - Passcodes are sent to the users' mobile device

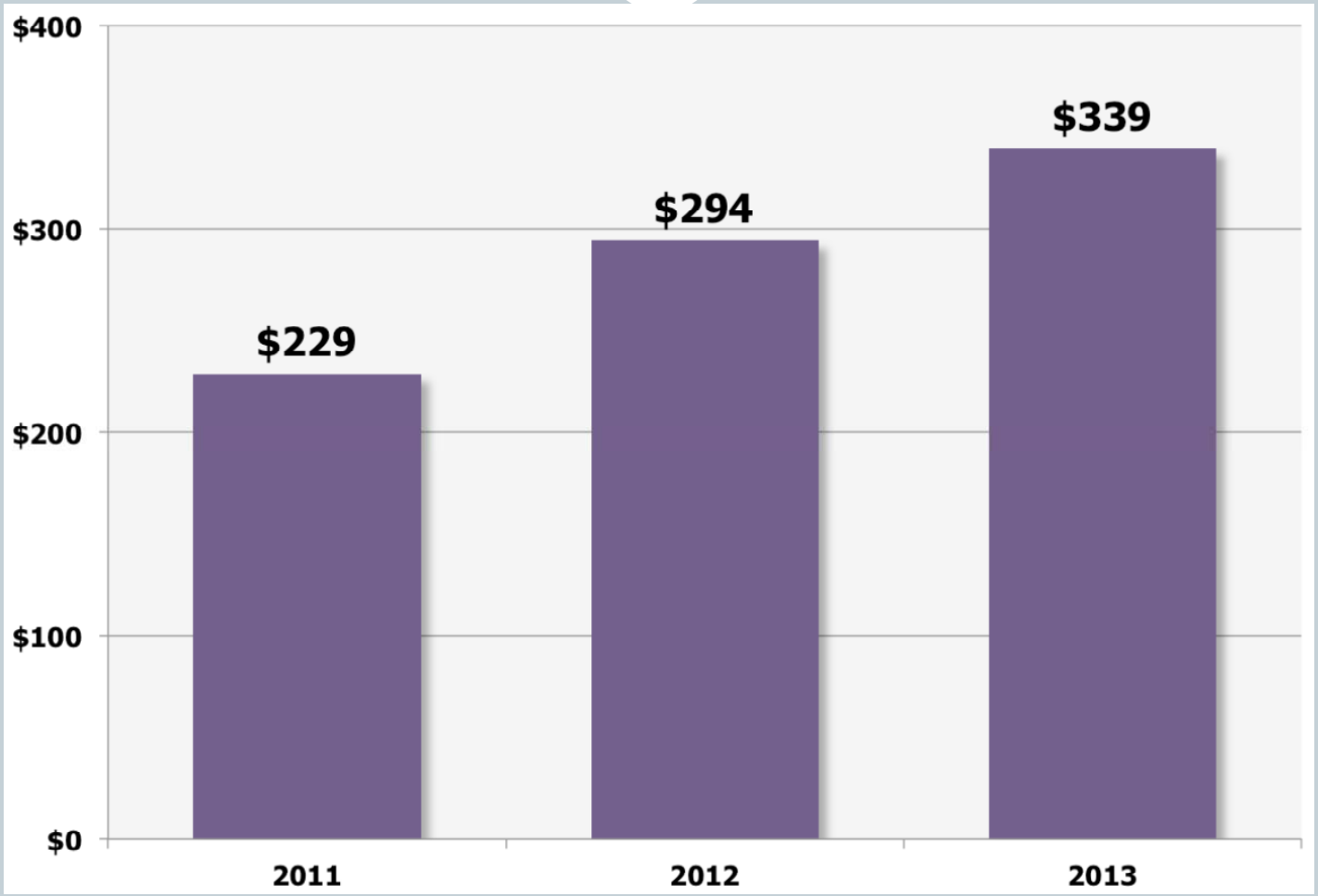
Mobile Device Management (MDM)

- More than 80 vendors serve this market (Osterman, 2012)
- Multiple platforms
- Cloud based SaaS, in-house server based, hardware appliance
- Encryption policy (phone, SD card)
- Lockdown security (camera, Bluetooth, Wi-Fi)
- Password enforcement
- Remote lock and wipe
- App inventory, distribution, blacklist
- Certificate distribution
- Lost phone recovery (locate and map)
- Configure email and contacts
- Configure Wi-Fi and VPN profiles
- Detect/restrict jailbroken or rooted equipment
- Selectively wipe corporate data, preserve personal data

Call for Cloud-based MDM

- As higher-end MDM products creep into the marketplace, with them comes increased complexity to learn and use, putting further pressure on IT
- As the percentage of smartphones in the enterprise continues to increase there are more devices to actively manage overall
- Full-time equivalent (FTE) staff requirements to manage smartphone users are increasing, from a median of 2.9 FTE staff member per 1,000 smartphone users in 2011 to 3.6 today and 4.0 in 2013 ($339k annually per 1000 phones)
  - $229 in 2011
  - $294 in 2012
  - Projected increase to $339 per user in 2013
  - 48% increase in 2 years largely due to BYOD

Annual Labor Cost per Smartphone User



Call for Cloud-based MDM

- 31% of organizations switching to a new MDM platform said they would likely select a cloud-based solution
  - 55% of those respondents said they would choose a private cloud solution for security reasons
- All of the reasons cited by respondents for an interest in cloud-based solutions are also directly applicable to managed services provider (MSP) solutions
  - Simplified administration and maintenance (69%)
  - Reduced and predictable costs (39%)
  - Improved security (39%)
  - Desire not to use internal IT staff to service MDM (21%)
- Currently, 15% of MDM implementations are provided from the cloud

MDM Pricing

- Cloud based services cost around $60 per device per year, but expected to drop by 50% over the next few years (Rubens, 2012)
- Airwatch:
  - $3.25 a month with no maintenance fee or $50 one-time fee with a $10 annual maintenance fee
  - Cloud is $.75 a month
  - Hardware appliance is one-time $5000 fee
  - Extra fees for cloud storage
  - Equates to $48 a year if paid monthly
  - Equates to $19 a year if the one-time $50 fee is paid

Managed Service Provider (MSP)

- Per device, per user, and tiered (gold, silver, bronze) pricing models
- A move from per device pricing model to a per user pricing model to cover all devices (e.g. PC, tablet, mobile device)
- Pricing survey results per device (US): *Kaseya (2011)*
  - Break Fix: $100/hour
  - Ongoing Desktop Support: $65/month
  - Ongoing Server Support: $216/month
  - Mobile Device Support: $21/month

  - ***Note: Specific services not listed***

Increased Risk for SMEs

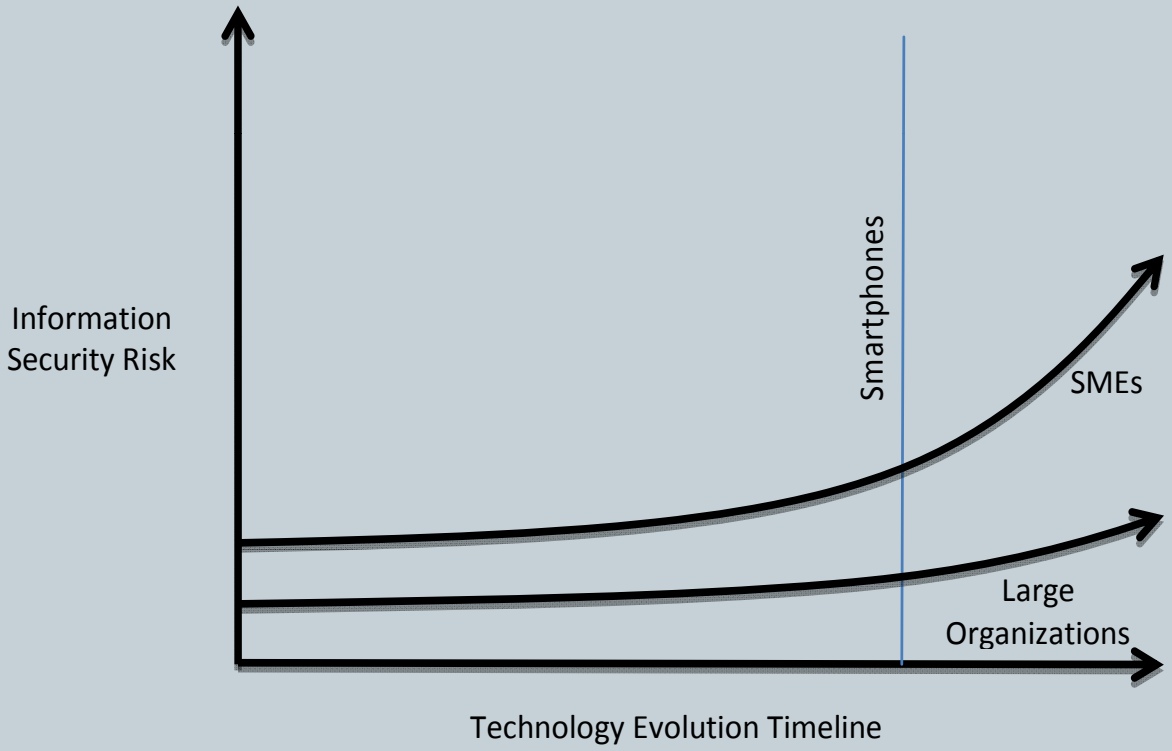


Figure 2

Potential Competitive Loss for SMEs

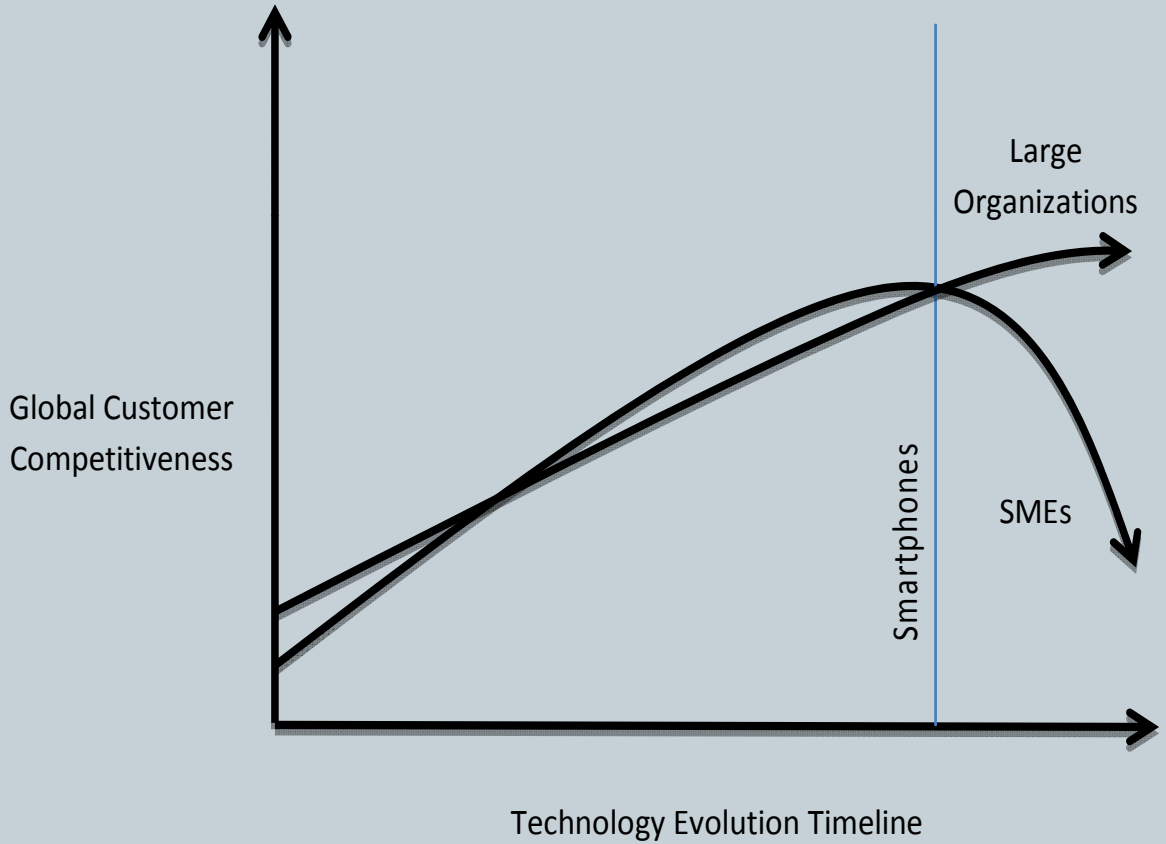


Figure 1

On-going Research

- SME awareness, concerns, actions of new security risks
  - How do they handle Wi-Fi concerns?
  - How do they handle Smartphone and tablet security concerns?
  - Will they implement MDM?
  - Will they use a MSP?
- Building on earlier SME security studies
  - Stand-alone PCs and Dial-up Internet (Bradbard, et al., 1990)
  - HI-speed Internet and WiFi networks (Johnson & Koch, 2006)
- SME recommendations and solutions.

Questions?