BYOD AND MOBILE DEVICE SECURITY

Ashish Jain, CIA
IT Audit Manager
Boston College

AGENDA

- BYOD benefits
- Threats to mobile devices
- Threat causes
  - Why we are concerned?
- What are the challenges?
- BC approach
- Best practices and solutions
- Policy considerations
- Audit perspective

MOBILITY IS PERVASIVE

- Around 44% of knowledge workers telecommute at least once a week
- 78% of white-collar employees use mobile device for work
- Average # of connected devices will increase from 2.8 to 3.3 by 2014
- 50% noted that their organization is implementing a desktop virtualization strategy

Source: Cisco IBSG 2012 Survey

Knowledge workers – who uses knowledge at work

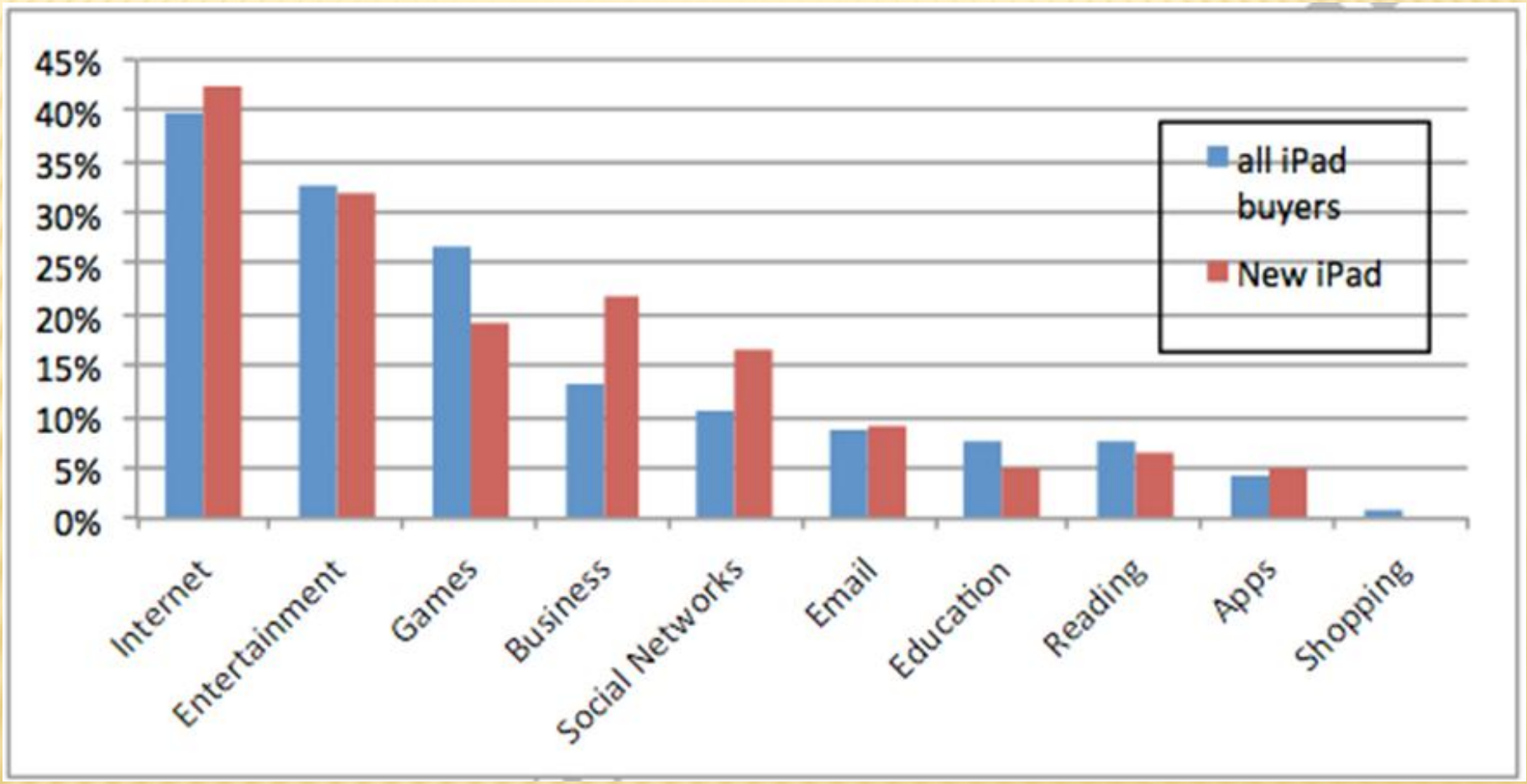
Picture source: theboldsoul.lisataylorhuff.com

BYOD BENEFITS

- Improved productivity
- Greater job satisfaction
- Greater mobility (work and personal time)
- Saving for IT department from maintenance and support load
- Opportunities for desktop virtualization

Pictures: zboostyourbusiness.com and leveltendesign.com

IPAD USE



Source: CIRP's surveys of 1,000 consumers. New iPads in Dec 2011- April 2012.

TOP THREATS TO MOBILE DEVICES

- Loss or theft of device
- Phishing
- Malware and viruses
- Spyware
- Worms
- Spoofing

WHAT IS AT STAKE?

- Loss of confidential data, e.g., SSNs, personal and student information such as grades, credit card, and account numbers.
- Intellectual property, e.g., inventions
- Research data
- Business confidential, e.g., alumni information

CAUSES

- Lack of policies and procedures for mobile devices
- Difficult to enforce policies and procedures
  - Educational environment
  - Personally owned device
- Most don't know all sources of confidential data and who has this kind of information
- Lack of initiatives and authority

CHALLENGES

- Who owns data on mobile devices and is there a strategy to get it back?
- Do you have authority to put in place desired policies and procedures?
- Do you have list of approved apps?
- What is your malware and antivirus strategy?
- Have you identified what really needs to be secured?

CHALLENGES

- Understanding what users do and want
- How to enforce password?
- What is your strategy if device is lost or stolen?
- Difficulties in reviewing and understanding voluminous amounts of log data
- How to ensure that devices are updated to latest firmware?

Developing an Approach for Mobile Device Security

THINGS TO CONSIDER

- Understand what users want
  - Only minimal headache
  - Security for their personal data
- What do we really need to secure?
- Cost vs. benefit analysis
- Various layers of security

OUR APPROACH

- Device activation is required and MAC address is stored.
- If issues are found,
  - deactivate or isolate the device
  - limit access where device does not have access to data (manual process).

BEST PRACTICES

- Risk management and policies
- Track MAC address
- User authentication at every login
- Clean devices periodically and at disposal
- VPN use or remote log-in
- Web-based access
- Use log data for your leverage; analyze log data to identify patterns or suspicious activity

POLICY CONSIDERATIONS

- Password or pin
- Remote wipe or may be remote disable
- Restrict “jailbroken” or “rooted” devices
- List of apps to avoid
- Make recommendations on device selection
- Mobile data protection (MDP), network access control (NAC), and mobile device management (MDM)
- Support structure for mobile devices
- Malware, virus, spyware protection

AUDIT CONSIDERATIONS

Risk-based approach. Common topics:

- Risk management and security policy
- Device management and tracking (remote wipe, device provisioning and deprovisioning)
- Access Controls (authentication, ports, separate process based on data on the device)
- Data Security (encryption, data retention, and data transfer)

AUDIT CONSIDERATIONS

- Malware and virus protection
- Secure transmission (VPN, Internet Protocol Security)
- Employee awareness and training
- Foreign device authorization and authentication process
- Monitoring of logs
- Problem identification and resolution procedures

WRAP-UP

"Dad, I've been hired online and asked to work from home. Today I need you to be "James Underhill, Director of Business Analysis."

Source: modernanalyst.com

Source: cloudtweaks.com

Questions?

CONTACT INFORMATION

Ashish Jain, CIA

IT Audit Manager

Boston College

Ashish.jain@bc.edu

617-552-4336