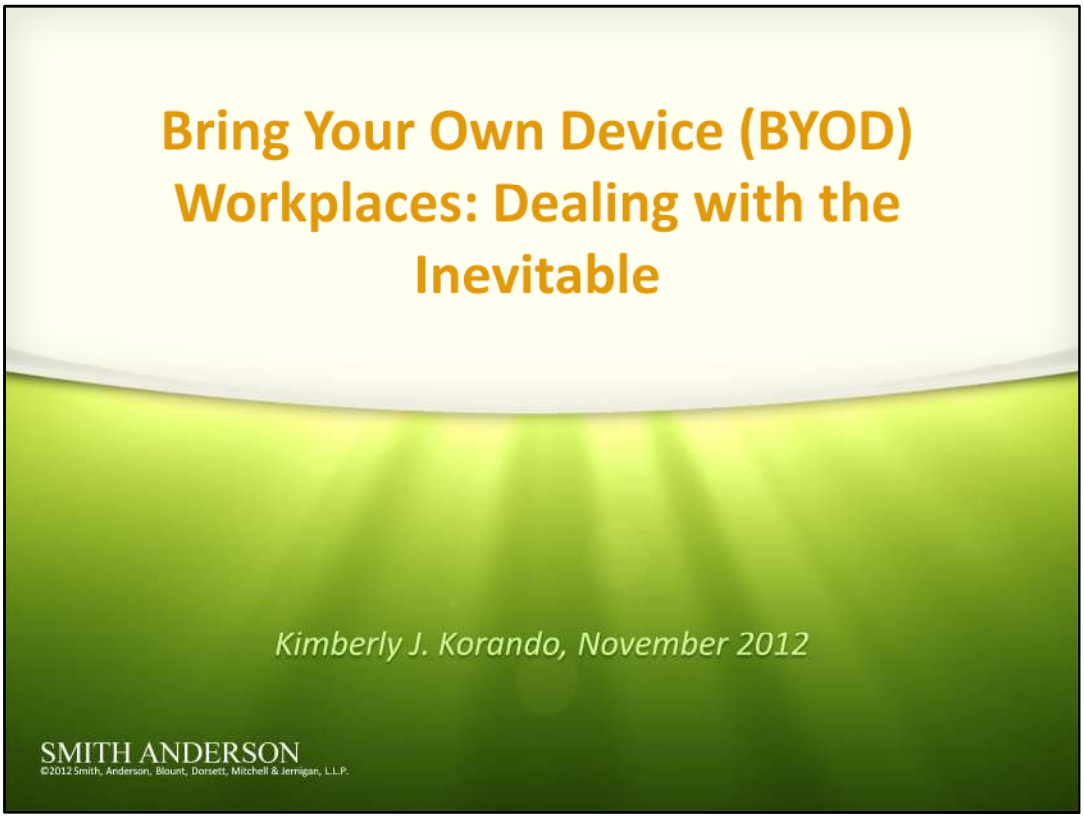
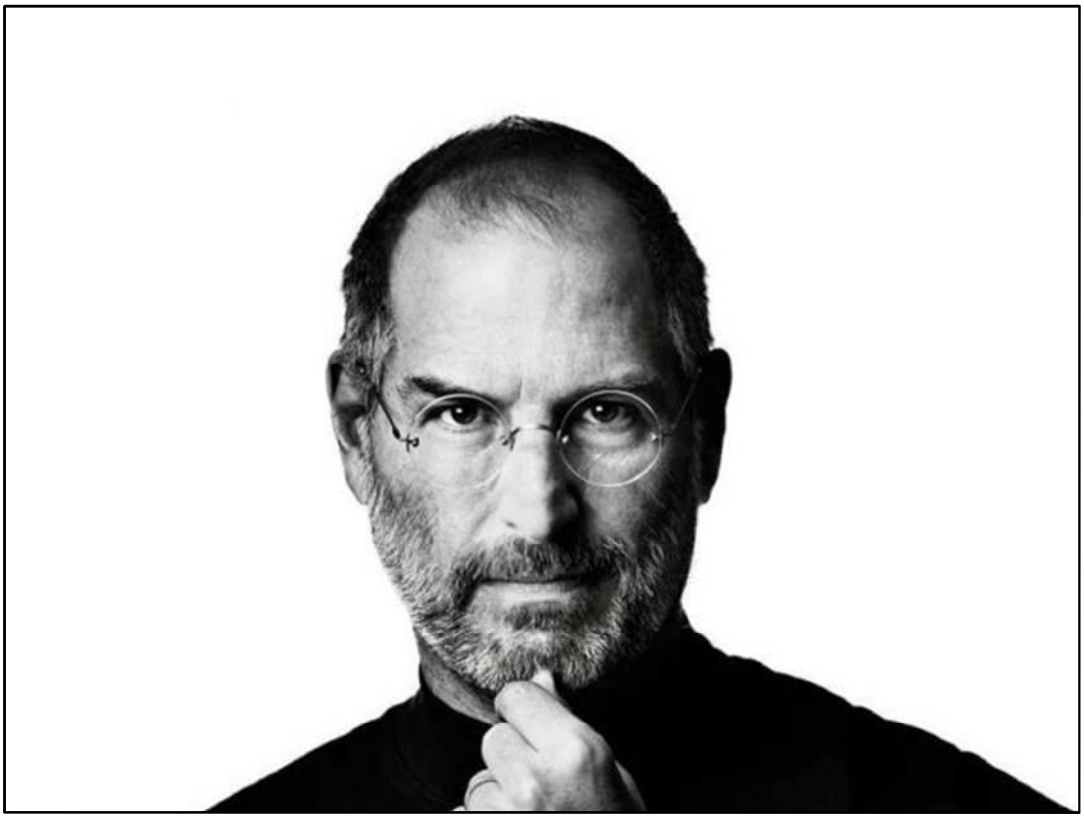
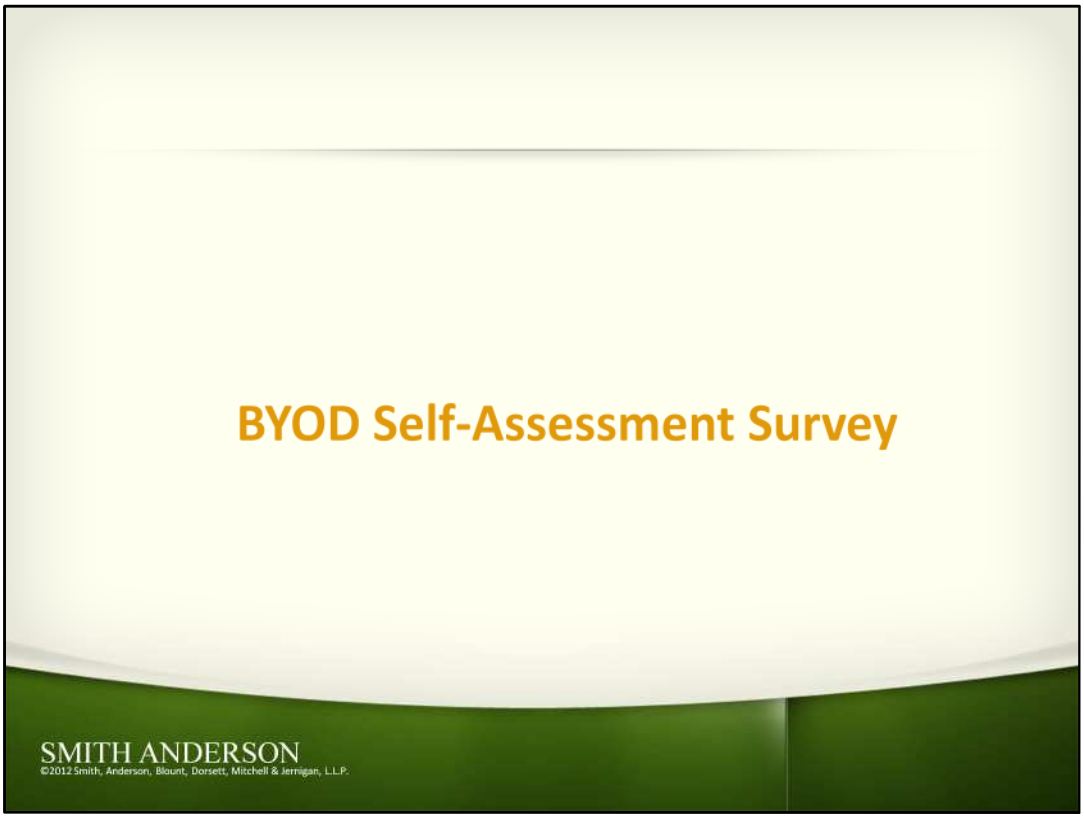
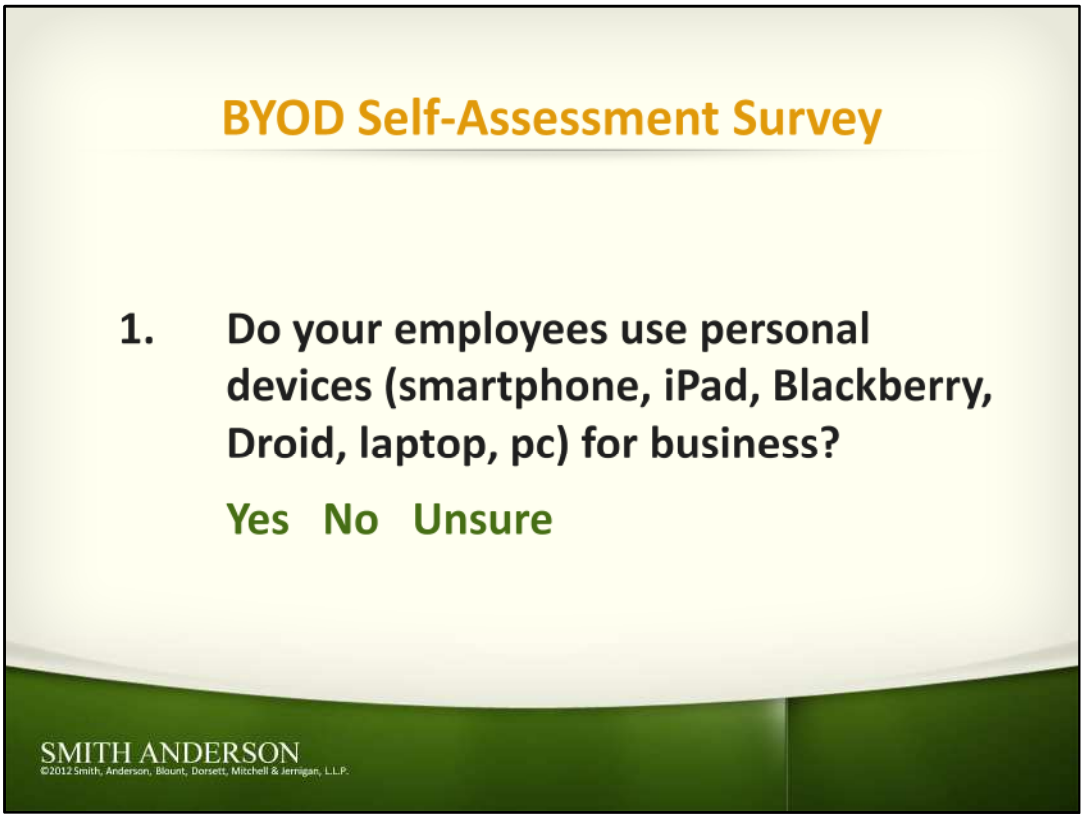
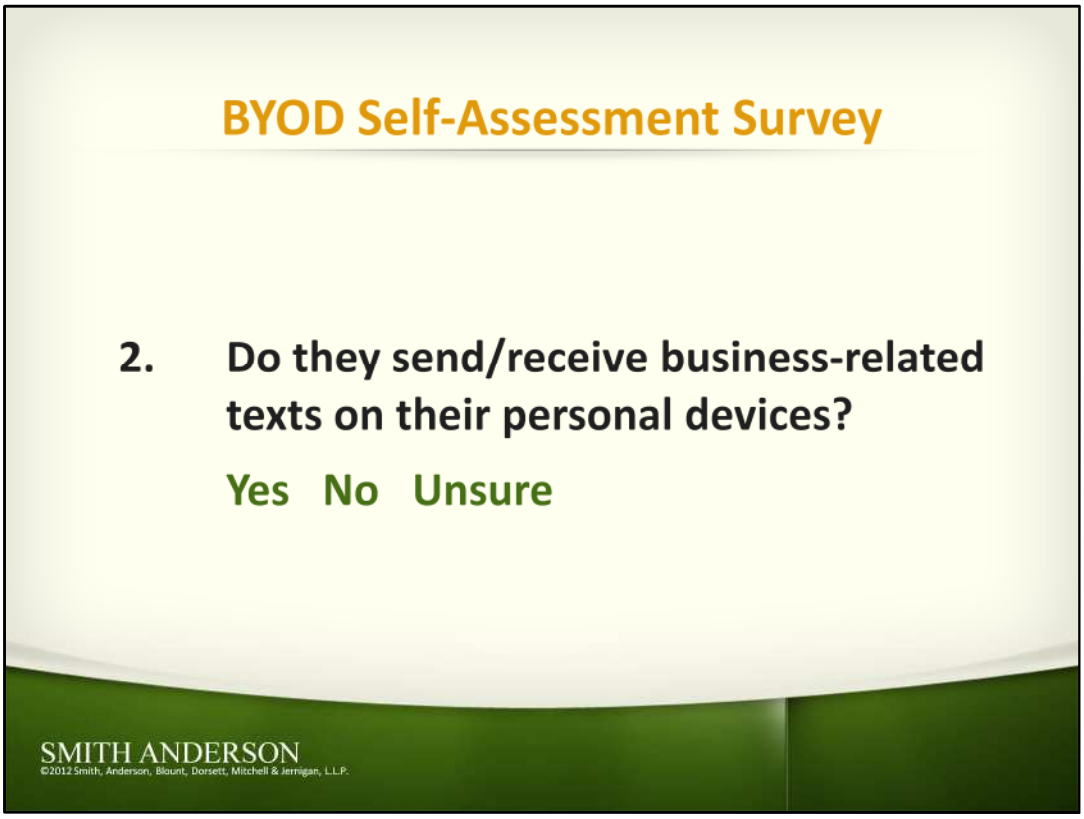
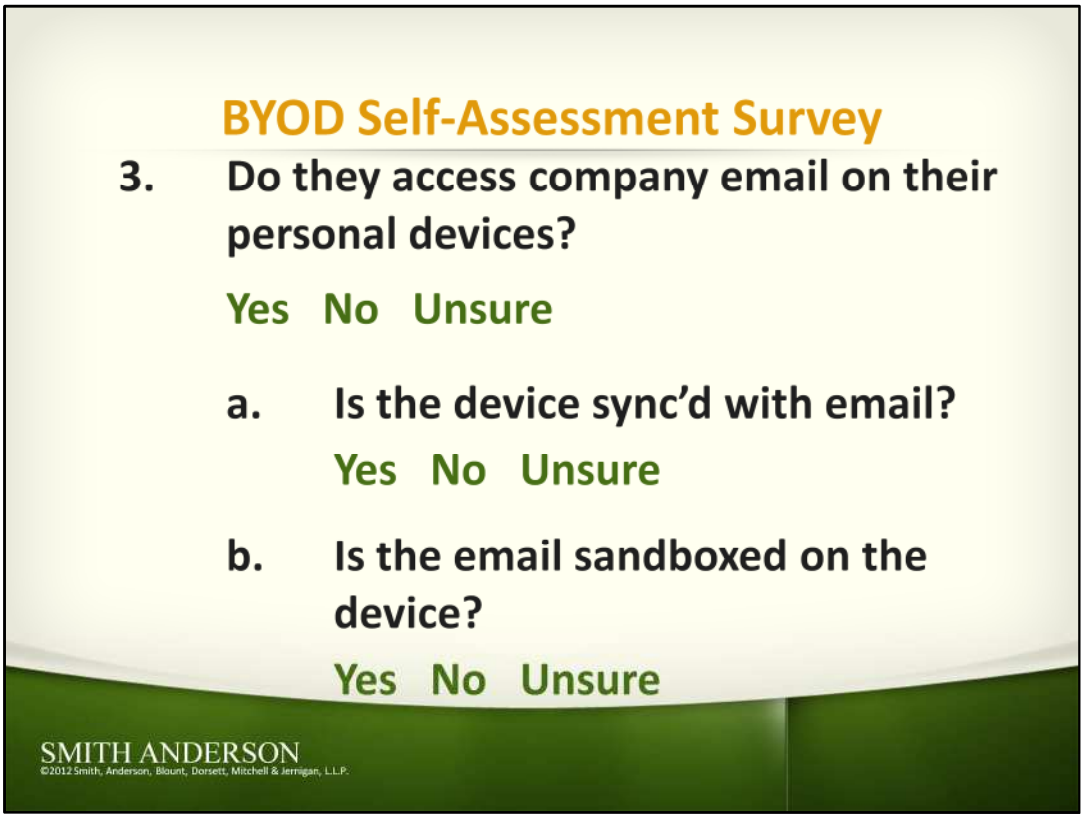

Bring Your Own Device (BYOD) Workplaces: Dealing with the Inevitable
Kimberly J. Korando, November 2012
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.

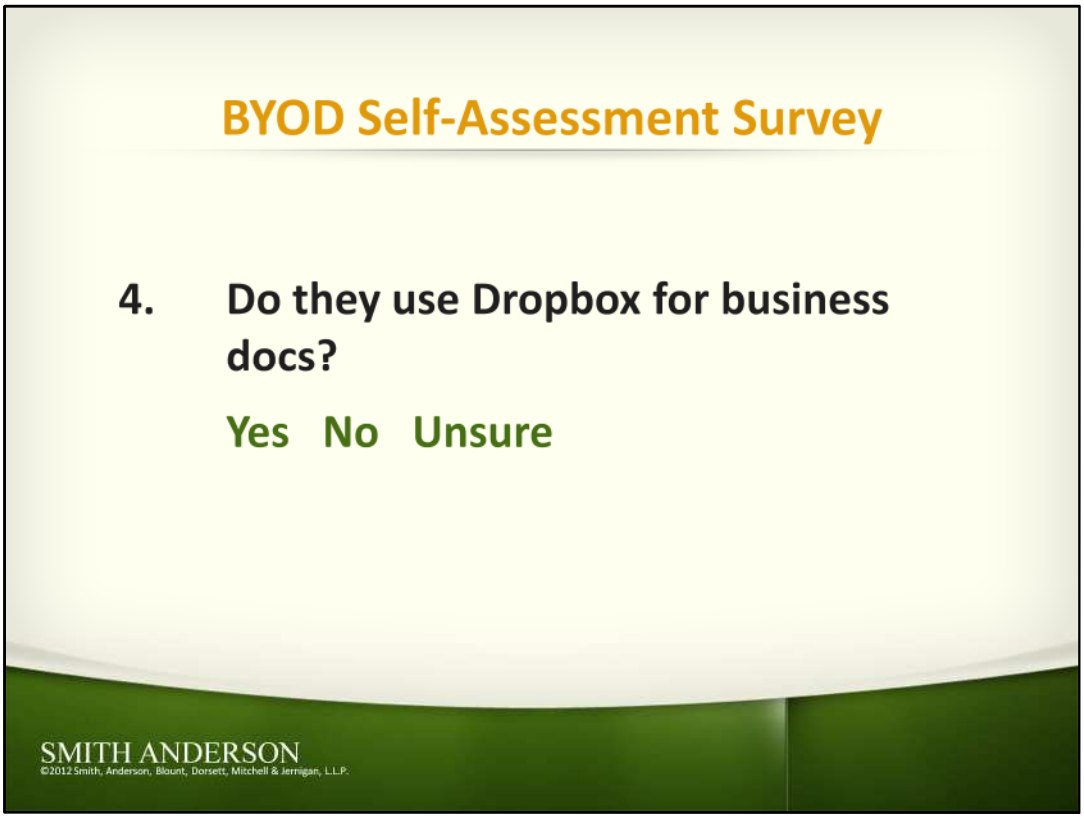


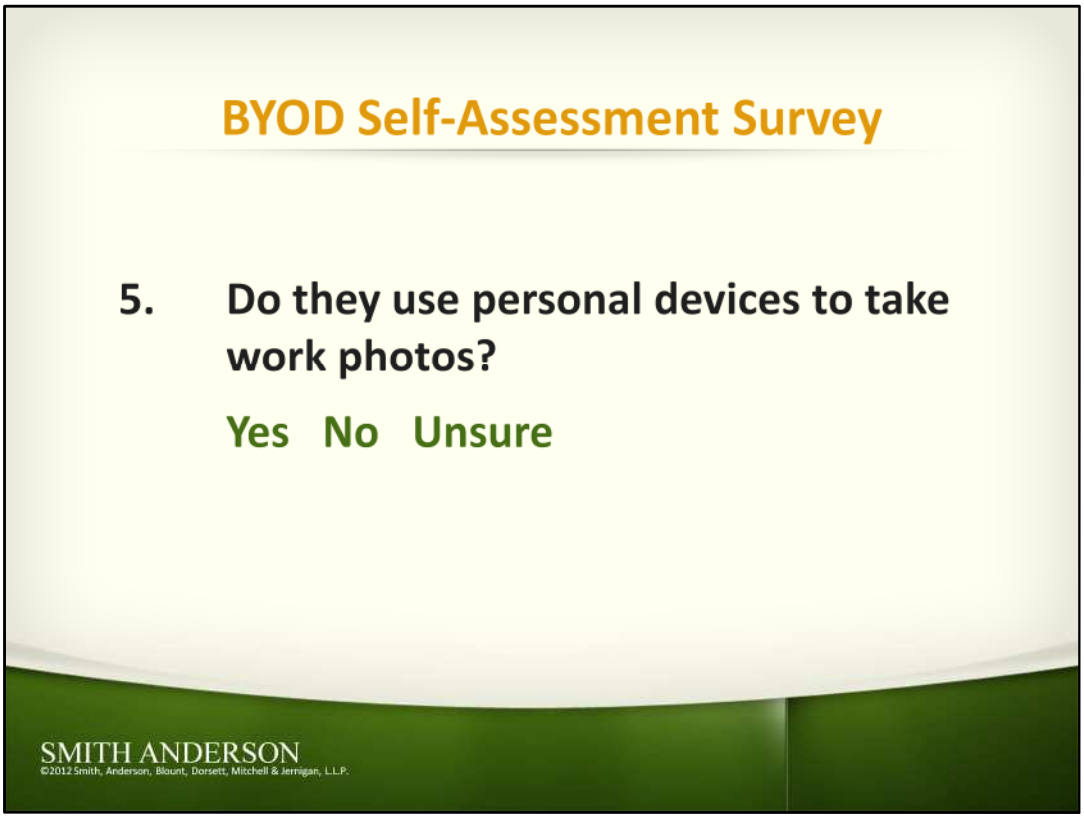

BYOD Self-Assessment Survey
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.

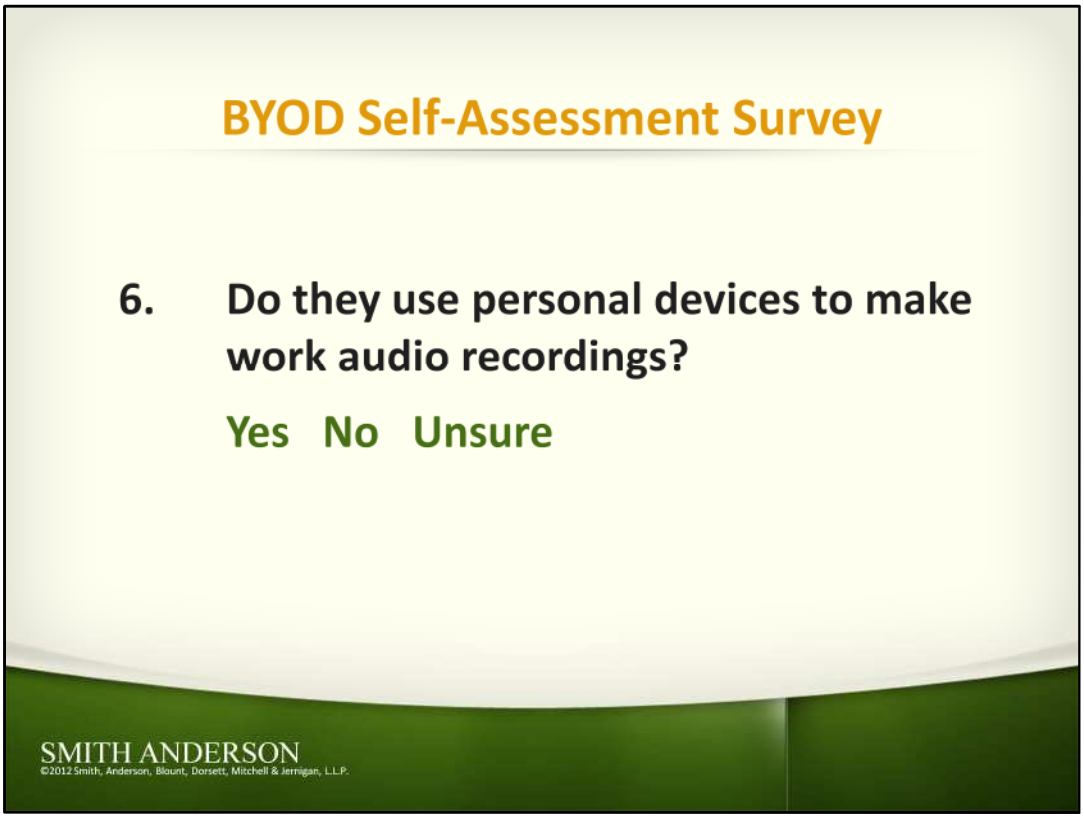

BYOD Self-Assessment Survey
1. Do your employees use personal devices (smartphone, iPad, Blackberry, Droid, laptop, pc) for business?
Yes No Unsure
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.

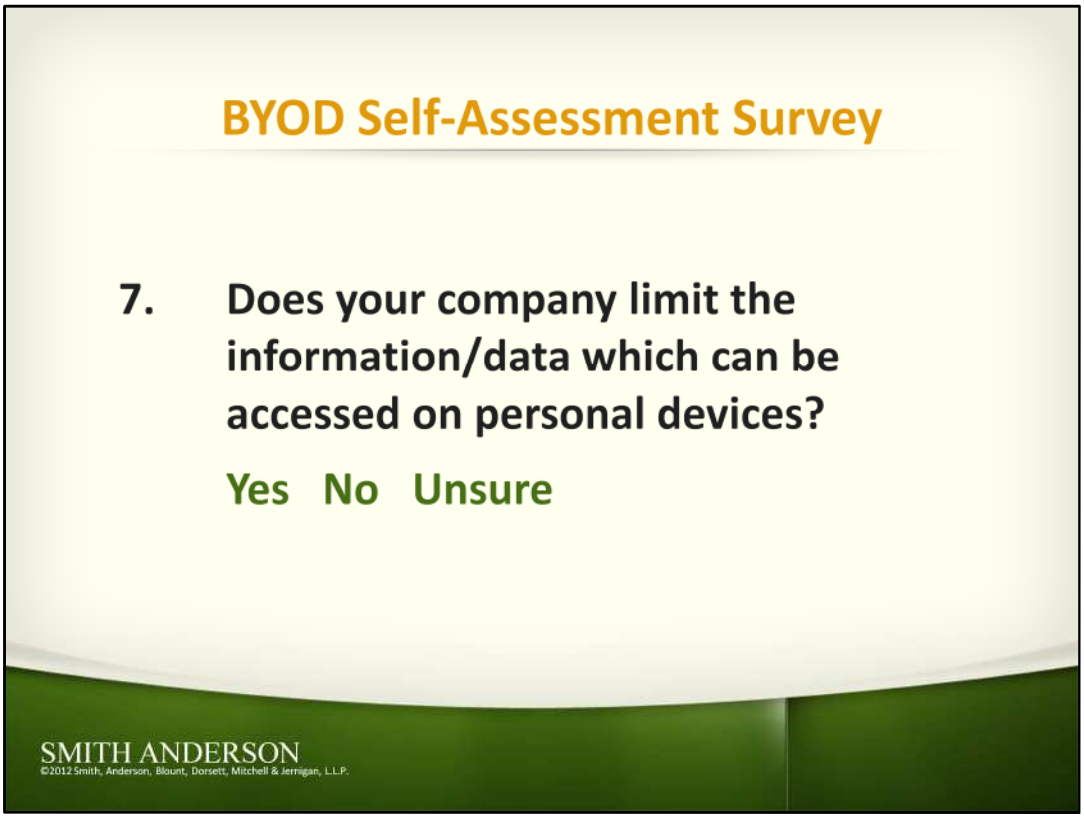

BYOD Self-Assessment Survey
2. Do they send/receive business-related texts on their personal devices?
Yes No Unsure
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.

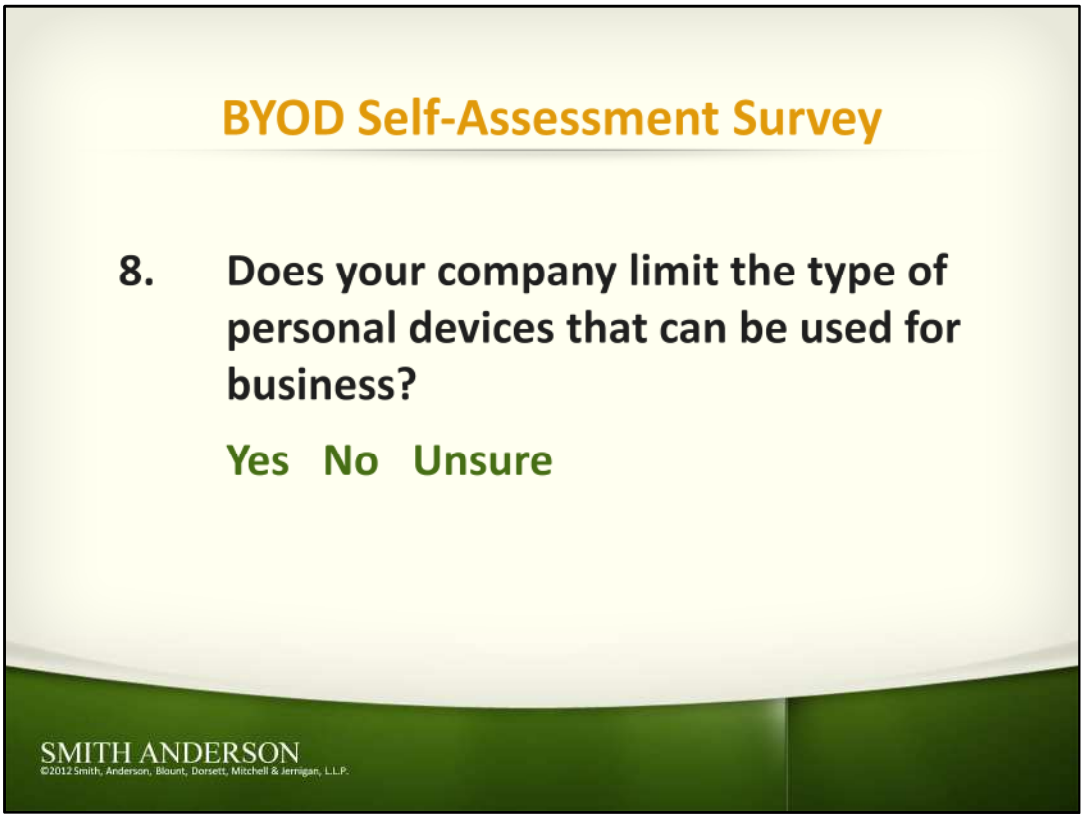

BYOD Self-Assessment Survey
3. Do they access company email on their personal devices?
Yes No Unsure
a. Is the device sync'd with email?
Yes No Unsure
b. Is the email sandboxed on the device?
Yes No Unsure
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.

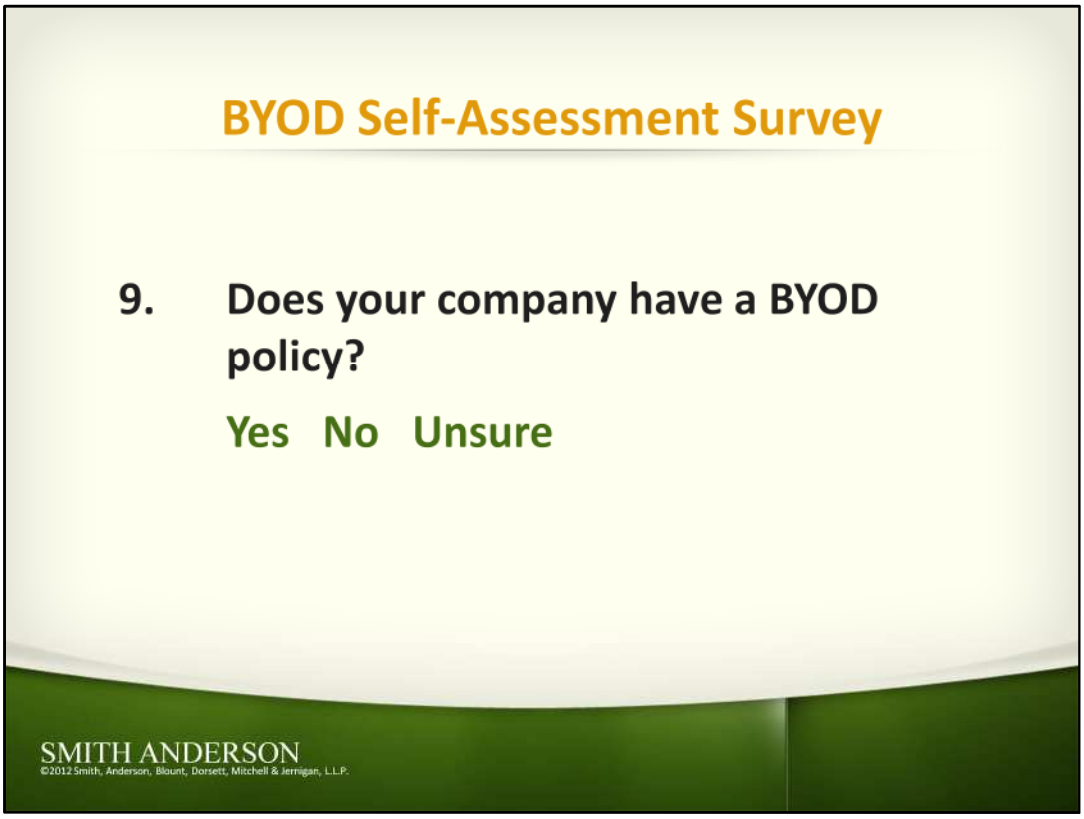

BYOD Self-Assessment Survey
4. Do they use Dropbox for business docs?
Yes No Unsure
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.

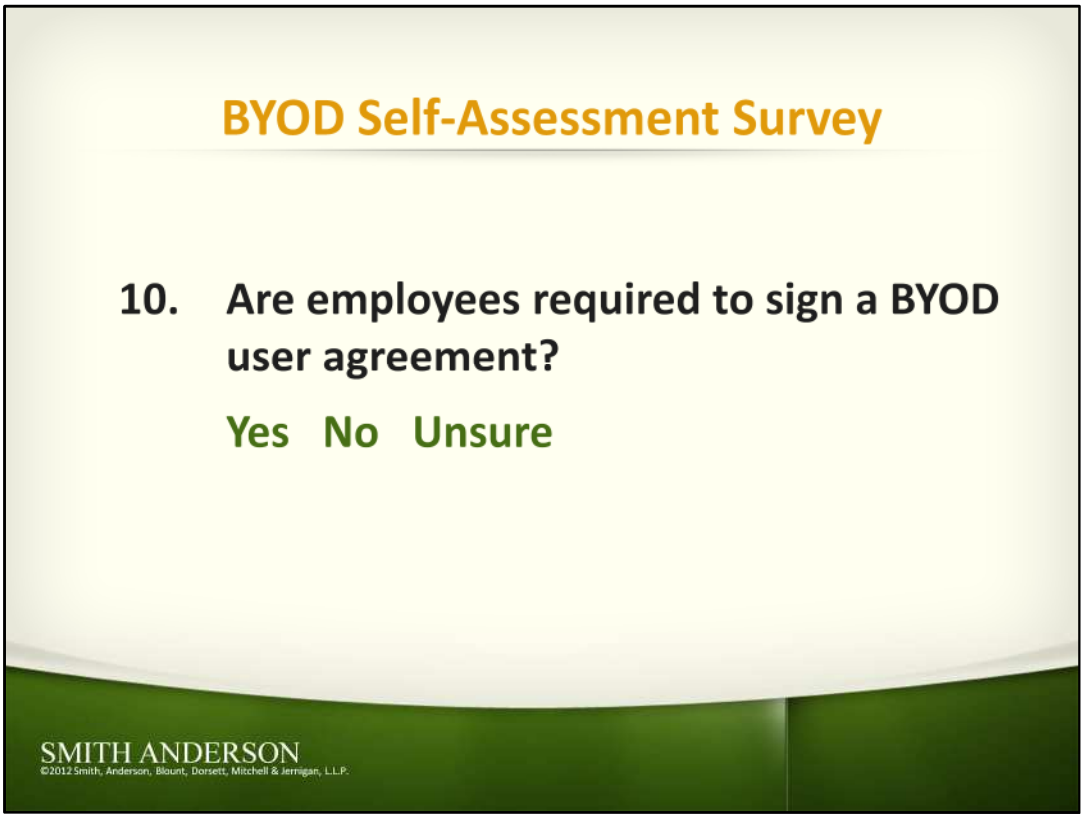

BYOD Self-Assessment Survey
5. Do they use personal devices to take work photos?
Yes No Unsure
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.

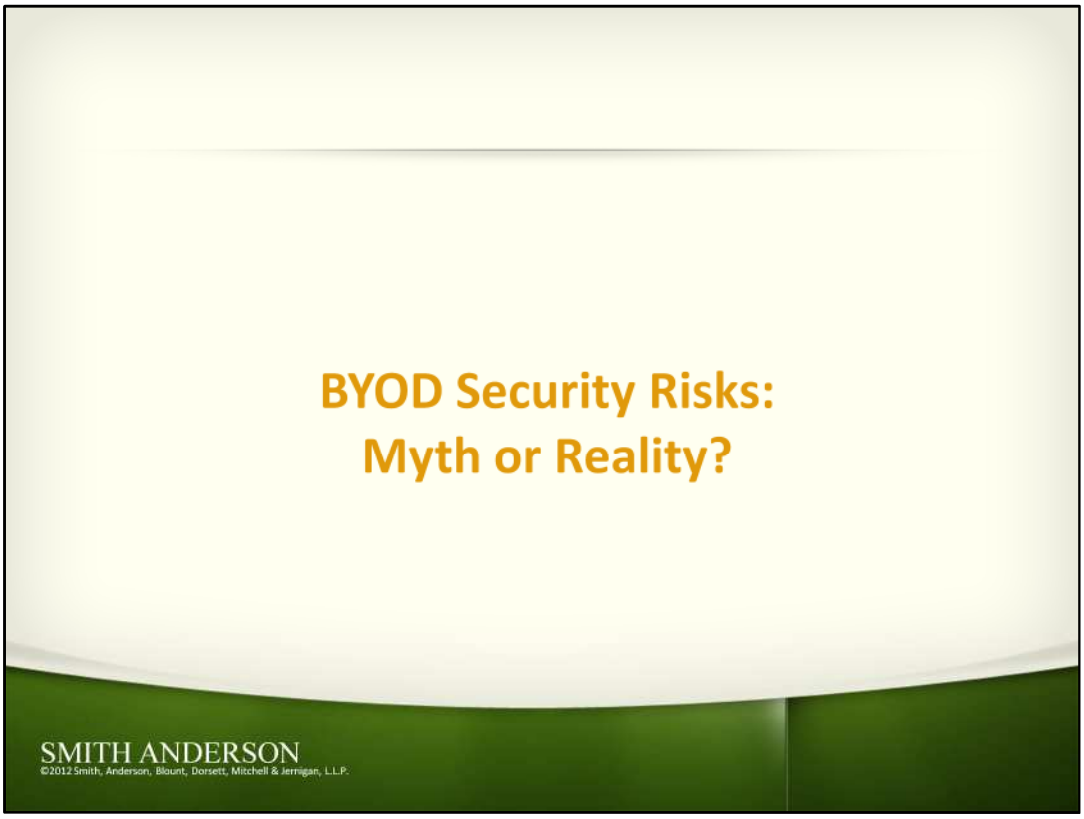

BYOD Self-Assessment Survey
6. Do they use personal devices to make work audio recordings?
Yes No Unsure
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.


BYOD Self-Assessment Survey
7. Does your company limit the information/data which can be accessed on personal devices?
Yes No Unsure
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.


BYOD Self-Assessment Survey
8. Does your company limit the type of personal devices that can be used for business?
Yes No Unsure
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.

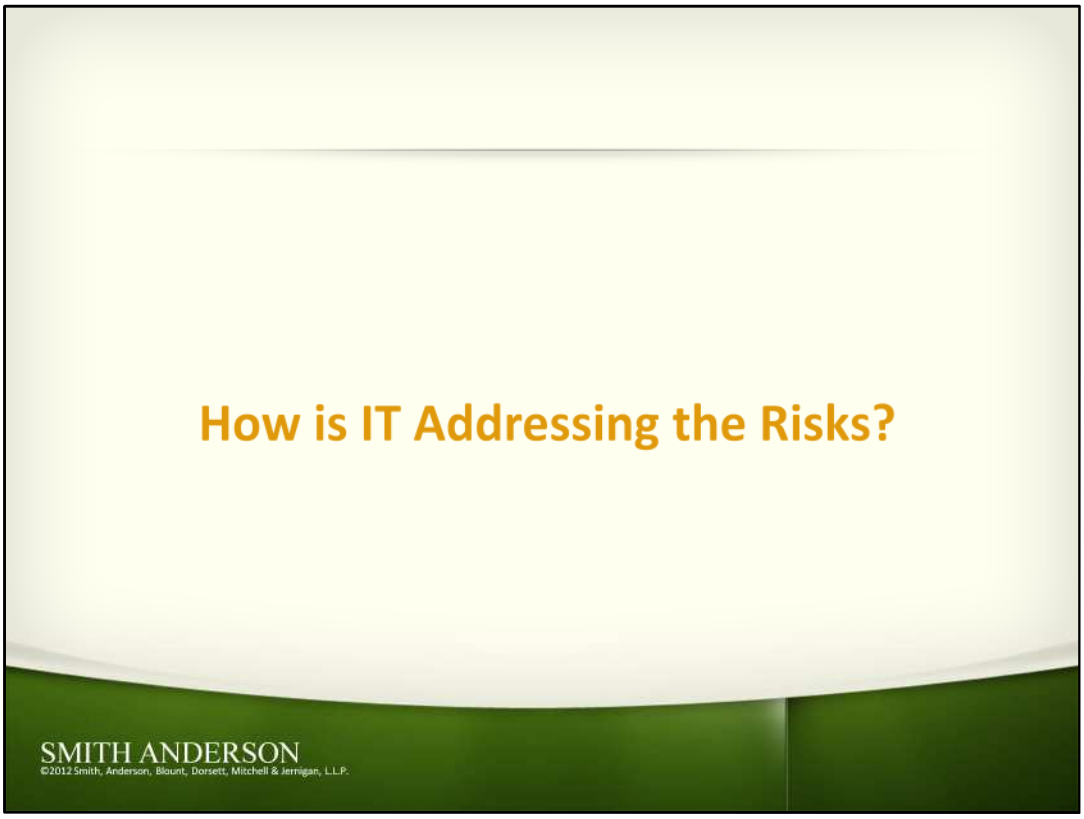

BYOD Self-Assessment Survey
9. Does your company have a BYOD policy?
Yes No Unsure
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.


BYOD Self-Assessment Survey
10. Are employees required to sign a BYOD user agreement?
Yes No Unsure
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.



BYOD Security Risks—Myth or Reality?

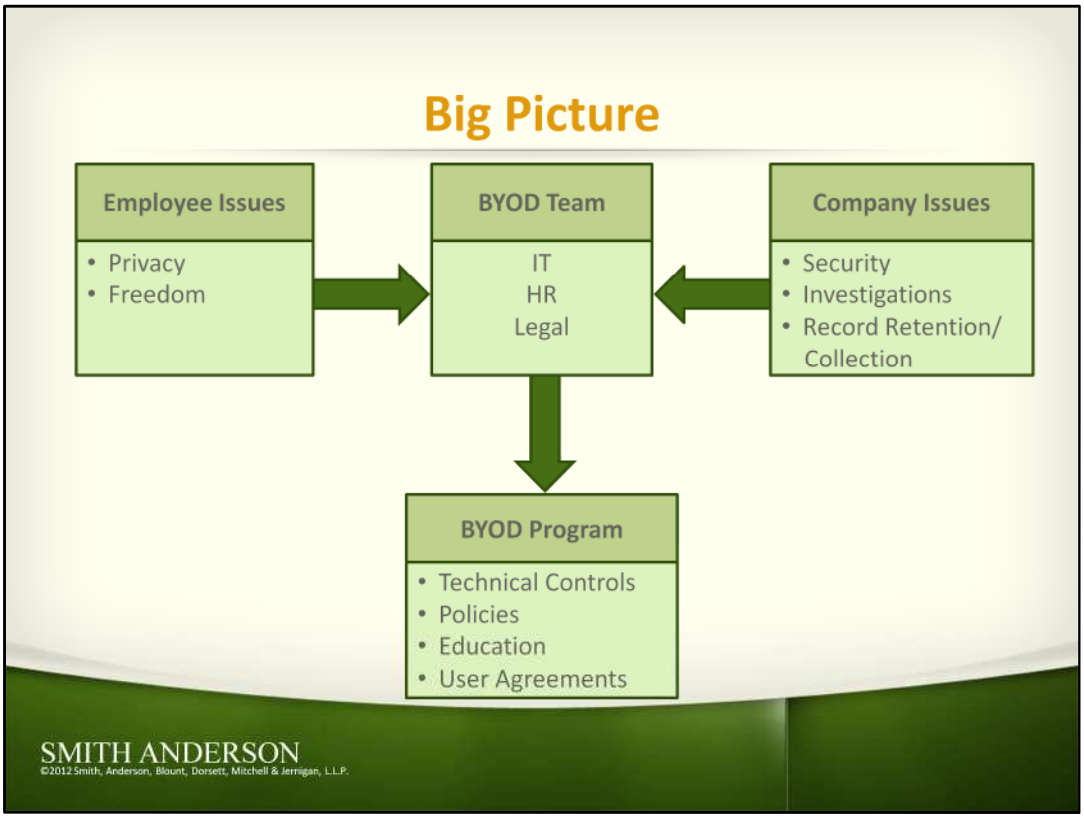
- Loss of technical controls (e.g., systems requirements, encryption, patches, monitoring, wiping, etc)
- Personal use riskier (e.g., personal activities can expose data to greater risks)
- Different devices, different levels of security risk
- The Cloud (applies also to company devices)

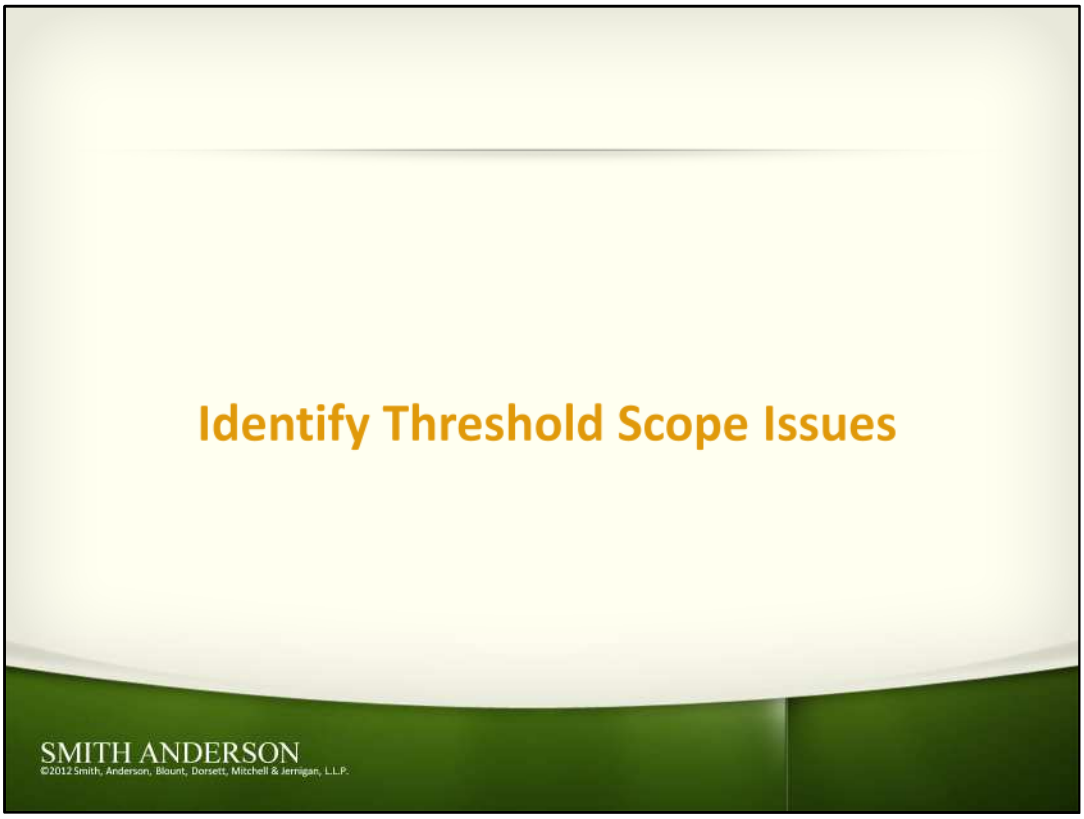


How IT Addresses

- Mobile Device Management (MDM) programs
  - Sandboxing
  - Remote wiping
  - Encryption
  - Password enforcement
  - Device tracking
  - Application management

Technical controls are not complete solution; need policy controls, too


Big Picture
Employee Issues
• Privacy
• Freedom
BYOD Team
IT
HR
Legal
Company Issues
• Security
• Investigations
• Record Retention/ Collection
BYOD Program
• Technical Controls
• Policies
• Education
• User Agreements
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.



Identify Threshold Scope Issues. For example:

a. What data/information will be accessible on BYOD devices?

   i. Trade secrets or other proprietary or highly confidential information that require special protection measures to qualify for protection under trade secret and related laws? Trade secrets laws typically require that the organization prove that it took "reasonable measures" to protect the information.

   ii. Data/information that is regulated by federal/state privacy laws (e.g., financial information, health information, personal identity information)?

b. Will BYOD be available to all employees or are some excluded (e.g., senior executives, R&D, sales, non-exempt, contingent, international workers, unionized workers)?

   i. Will different approaches be taken with employees who have access to highly confidential or other protected information?

c. Will there be limitations on the types of permissible BYOD devices?

   i. Factors to consider include security issues with particular devices, IT ability to support or collect data from particular devices/operating systems.

   ii. Will the organization provide helpdesk support for BYOD devices? If not, what security precautions will need to be taken to protect company information from third party vendors?

d. Will BYOD be mandatory or a privilege?

   i. Employees are more compliant with BYOD programs that are a privilege as opposed to those that are mandatory.

Policy Controls

a. Policy decisions will be based on a number of factors, including the type of employees, the type of data and degree of confidentiality, company's acceptance of risk.

b. Decide whether a separate stand alone policy will be issued or existing policies revised to address BYOD.

   i. Stand alone policy should properly cross-reference other related policies.

c. Address Security provisions. Examples to consider:

   i. Require compliance with all security procedures (e.g., encryption, passwords, anti-virus software, no upgrades unless company approved, no syncing or unauthorized back-up or storage, no disabling security or other systems).

   ii. Compliance with "required/prohibited" app list, prohibited/acceptable devices, prohibited jailbreaking/modding devices, no shared use of devices (unless company information is sandboxed), no "clouds" (e.g., Dropbox, Evernote).

      A. Under federal Stored Communications Act, the company may not be able to get its data back from employee's "cloud" account.

      B. This issue also applies to company-owned devices.

Policy Controls (cont.)

d. Address Privacy provisions. Examples to consider:

   i. What expectation of privacy will employees have to data (company and personal) on personal devices?

   ii. Will activities that are prohibited on company devices (e.g., viewing pornography) be prohibited on personal devices?

   iii. What monitoring will be done (e.g., company network, data transmission, on device)?

   iv. How will the company protect against employees bringing another party's (e.g., former employer) information into the "workplace"?

e. Ensure that policy and user agreement includes requirement that device be forfeited to company and all data (including personal data) copied in the event of internal investigation/record preservation/eDiscovery.

f. All other policies apply when personal device used on work time or premises .

g. Identify and revise other applicable policies, as needed (e.g., harassment, data privacy/security, time worked/reporting, confidentiality, record retention, computer use).

User Agreement

a. Policies without User Agreement are insufficient to protect the company because policies are not contractually binding on individual. Moreover, authority to use personal device should serve as consideration for agreement.

b. Recommended provisions include:

i. Policy compliance (spell out key requirements, prohibitions listed in Policy Controls above).

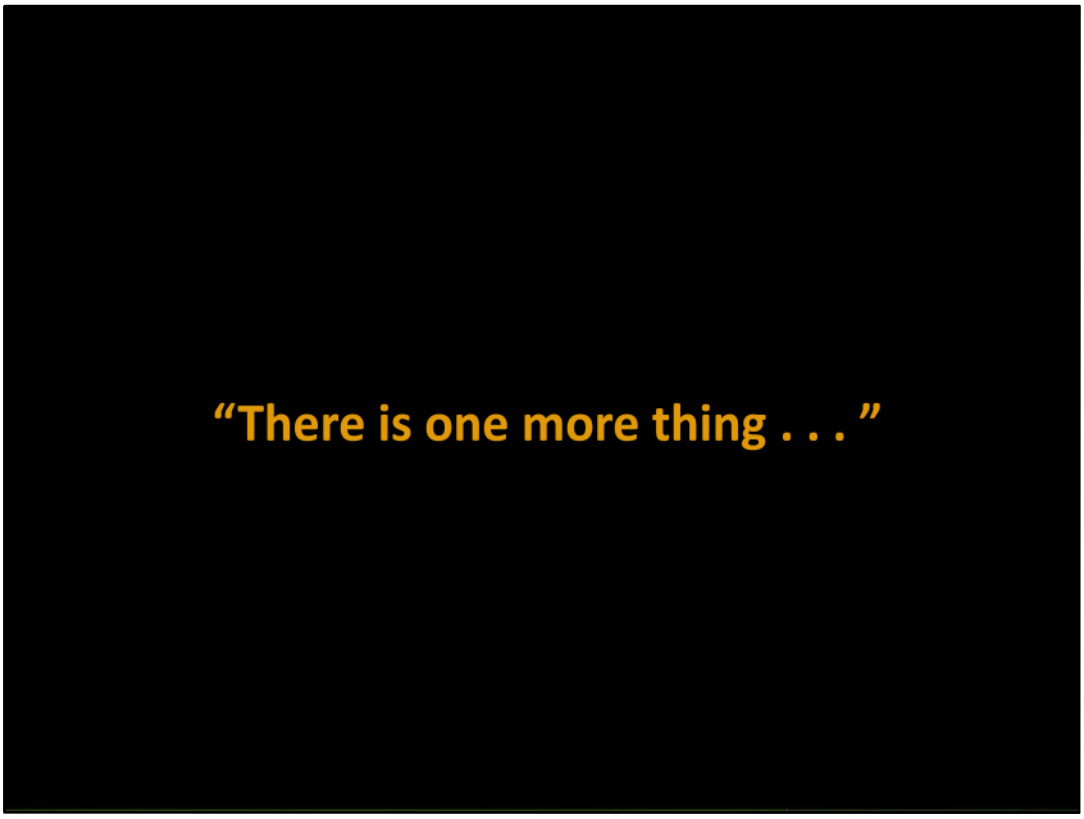
ii. Consent to company to install security software, monitor device, access (including provision of login credential), copy, wipe/brick, exit interview/inspection and wipe, device forfeiture on demand (access, copy, wipe also apply to personal information, especially in the event of litigation hold responsibilities or investigations).

A. If company information is not sandboxed and company does not have employee consent to wipe data, then company may be liable for destruction of employee's personal information that is wiped.

iii. Requirement that company data be retained until company can copy data, including back-up.

iv. Device disposal requirements.

v. Acknowledgement that company owns company information on personal device.



User Agreement

a. Policies without User Agreement are insufficient to protect the company because policies are not contractually binding on individual. Moreover, authority to use personal device should serve as consideration for agreement.

b. Recommended provisions include:

   i. Policy compliance (spell out key requirements, prohibitions listed in Policy Controls above).

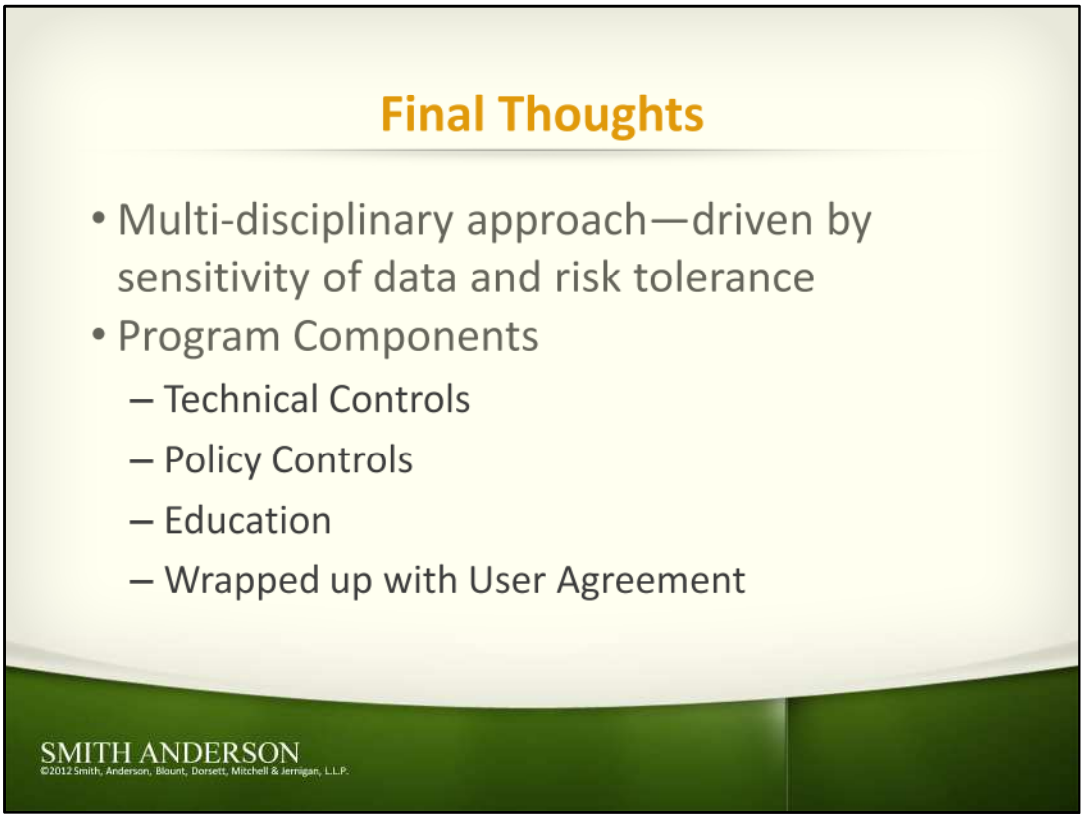
   ii. Consent to company to install security software, monitor device, access (including provision of login credential), copy, wipe/brick, exit interview/inspection and wipe, device forfeiture on demand (access, copy, wipe also apply to personal information, especially in the event of litigation hold responsibilities or investigations).

      A. If company information is not sandboxed and company does not have employee consent to wipe data, then company may be liable for destruction of employee’s personal information that is wiped.

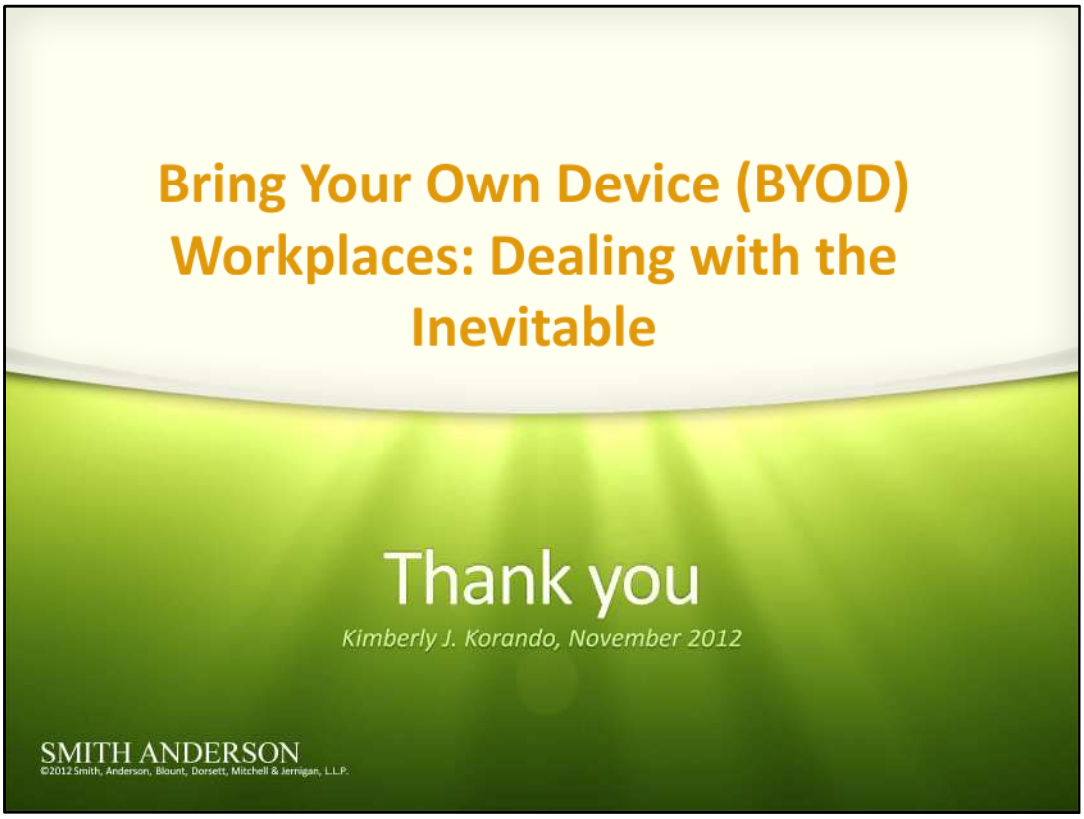
   iii. Requirement that company data be retained until company can copy data, including back-up.

   iv. Device disposal requirements.

   v. Acknowledgement that company owns company information on personal device.



See also Bring Your Own Device (BYOD) Program Checklist (attached).


Bring Your Own Device (BYOD) Workplaces: Dealing with the Inevitable
Thank you
Kimberly J. Korando, November 2012
SMITH ANDERSON
©2012 Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.