Has Your Financial Institution Embraced BYOD (Bring Your Own Device)?

Keiter
Your Opportunity Advisors

February 2013

The "Bring Your Own Device" trend continues to be a hot topic for companies as employees push for the ability to use their own smartphones, iPads/tablets, and computers. As with any decision, a financial institution that is considering or expanding beyond smartphones, a BYOD program must weigh the pros and cons. The pros can include improved productivity (accessibility) and higher employee satisfaction while cons include increased workload for IT departments, higher infrastructure and software costs, and more complex security. In fact, in a recent study released by MobileIron and iPass, *2013 Mobile Enterprise Report*, the top two sources of BYOD frustration for an IT department are onboarding and supporting an increasing number of differing devices. Implementing centrally managed Mobile Device Security and Mobile Content Management software can alleviate some of the IT department's frustrations.

For financial institutions considering BYOD programs, the following steps should be taken:

Implement a Policy.

- Implement a *Bring Your Own Device* policy. Here is a link to BYOD Policy Template.
- Employees should be required to sign and acknowledge their adherence to the policy.

Select and Implement a Mobile Device Security Solution.

- Identify your needs/requirements and determine the solutions that best meets the needs, within your price range.
- The solution should be able to centrally manage and control the security of the device to enforce corporate security policies and expedite the handling of secure lost, stolen, or retired devices.
- Require strong password controls on devices, including inactivity timeouts and lockout after failed login attempts.
- Configure devices for remote wiping (automatically) if excessive failed logins, lost, or compromised.
- Enable encryption on the device.

Select and Implement a Mobile Content Management Solution.

- Identify your needs/requirements and determine the solutions that best meets the needs, within your price range.
- The solution should be able to centrally manage and control the access, storing, and viewing of corporate documents.

While financial institutions always need to be cognizant of security risks, a well-controlled BYOD program can provide significant value to your institution. If you have not considered a BYOD program yet, it is time to put some thought into implementing one.

Contact Scott McAuliffe at smcauliffe@keitercpa.com or your Keiter Engagement Team for additional information on how your business may be impacted by BYOD.

Stay in touch

Information provided by Keiter is intended for reference only. The information contained herein is designed solely to provide guidance to the reader, and is not intended to be a substitute for the reader seeking personalized professional advice based on specific factual situations. This information does NOT constitute professional accounting, investment, tax or legal advice and should not be interpreted as such.

Although Keiter has made every reasonable effort to ensure that the information provided is accurate, Keiter, and its shareholders, managers and staff, make no warranties, expressed or implied, on the information provided. The reader accepts the information as is and assumes all responsibility for the use of such information. All information contained is protected by copyright and may not be reproduced in any form without the expressed, written consent of Keiter. All rights are reserved.

IRS Circular 230 Disclosure:
To ensure compliance with requirements imposed by the IRS, we inform you that any tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding any penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction(s) or tax-related matter(s) addressed herein.