3 Challenges and Tips for Mobile Device Adoption in Financial Services
Congratulations for taking the big step! You’re formalizing your mobile strategy with a new Bring Your Own Device (BYOD) policy at your financial organization, joining countless other companies doing the same thing.

Research firm Markets and Markets estimated BYOD adoption rates at 36% of businesses in North America at the end of 2016, a figure it projected to grow to 50% by the end of 2017. So, you aren’t alone.

Among banks, insurers and other financial services firms, it’s been consumers driving the mobile bandwagon so far. According to a 2015 U.S. Federal Reserve study, 94% of mobile banking customers had checked their account balances or transactions via a mobile device in the past 12 months. Similarly, 71% had downloaded their bank’s mobile app and 57% had received an alert from their financial institution via text message, push notification or email.

At the same time, an IDC survey of financial services providers in 2015 found that two-thirds of its respondents had yet to fully develop a policy for their own workplaces governing the use of mobile devices. That, most experts agree, is quickly changing. Financial services providers believe employee use of iPad®, iPhone® and other mobile devices will provide overall cost benefits as well as increased collaboration with their colleagues and customers.

Though many financial organizations might prefer their employees use company-owned mobile devices, studies show an overwhelming preference among millennials and others for using their own personal devices for business.

As Enterpreneur.com wrote in their article, “Employees Feel the Love When Companies Embrace BYOD,” employees feel being able to use their personal devices provides more freedom over how and where they work — an attractive recruiting perk in today’s competitive hiring market. Among the benefits cited in the article, “It also allows employees to work outside of the traditional workplace constraints, which is sometimes necessary (especially when late night inspiration hits).”

So today, many financial companies provide employees a choice of using corporate-owned and employee-owned devices. If your planned BYOD policy includes or augments a broader policy governing mobile device use overall, you’re taking the right approach.

This white paper seeks to give you more information about BYOD and mobility in financial services, including the challenges you may face, and some advice on how best to address them. We’ve boiled down these challenges to time, money and security (in no priority order; all can be equally difficult).

First Big Challenge: Time

Financial services organizations have been known to take up to a year or longer to implement BYOD or broader mobile device policies. It’s no surprise — mobile adoption comes with complex infrastructure, governance and resource challenges to overcome in an industry with massive data security and risk management concerns.

IT teams often bear the brunt of implementation, with projects such as:

- Updating company networks and security mechanisms to accommodate more mobile devices
- Hammering out BYOD policies that, among other things, address regulatory compliance standards such as the Graham Leach Bliley Act, the Sarbanes-Oxley Act, the PCI Data Security Standard and more
- Tracking, supporting and replacing mobile devices (especially employee-owned)
- Developing mobile apps for internal processes and project management systems
- Adding cloud services to provide more storage

Transitioning to a new enterprise mobility suite for mobile-device management (MDM) and mobile access adds to the timeline, and poor-performing solutions can throw everything off track. Imagine the complications when new mobile-device shipments are delayed or lost, devices are shipped to the wrong employees or don’t work right away, or devices are so slow in arrival that employees buy new ones on their own, disrupting asset tracking.

Tips for Saving Time

1. Find an IT solutions provider that offers full asset lifecycle management for your mobile devices. Having a single source to design, procure, ship, deploy and even decommission your mobile devices will help your organization avoid managing multiple invoices and procurement processes, and achieve greater accountability from your provider.

2. Invest in an enterprise mobility suite that includes:
   - An online portal for users with choices in devices, carriers and plans
   - Devices shipped directly to end users
   - Membership in the Apple Device Enrollment Program (DEP) for better tracking
   - Effective transfer of phone numbers, and ease in getting apps, data and network access squared away
   - Maintaining a level of security, compliance and cost control that mitigates company risk — high risks with any of these soaks up time as well as money

3. Use personas for developing internal mobile applications in an efficient, cost-effective manner. Start out with basic process needs, a narrow focus and a clear idea of how different mobile users will navigate the app. Add new features over time. Dedicate time for IT teams to do this work uninterrupted to avoid wasting time and money producing failed apps.
Second Big Challenge: Money

Obviously, since time is money, any challenge that drains time also exhausts money. But here are other key concerns tied largely to the wrong data plan:

- Being locked into long-term contracts with overage fees, wasted data and/or other penalties
- Excessive termination fees for cancelled contracts
- Data plans that don’t detail data usage per employee device, forcing an organization to try to do it manually or simply pay for unused data
- Inefficient telecom expense management — allowing billing for redundant services, unused devices and fraudulent charges

In addition, organizations lose money when they don’t take advantage of volume discounts in procuring devices, don’t attempt to remarket and resell their used devices, or use a service desk provider inexperienced in mobile support — i.e., have technical limitations when it comes to different operating systems or device types.

Tips for Saving Money

1. Sign up for a mobile access plan that attaches price-competitive rates to individual devices, with options for new devices and projects or for devices requiring more data or bandwidth. Steer clear of plans with early termination or activation fees.
2. Make sure your enterprise mobility suite enables users with flexible device options and self-service. This reduces your purchase of devices that go unused or used sparingly by employees who go out and get their own devices.
3. Consider a telecom expense management solution to minimize overspending and redundant costs.
4. Find a solutions provider that will purchase Apple® and/or other mobile devices at competitive prices, through effective sourcing management. Similarly, find a provider that also can offer money back for used devices, through refurbishment, remarketing and resell.
5. Don’t underestimate the importance of a well-planned and thought-out deployment phase. Mistakes here can lead to costly delays or budget overruns.
6. Be selective about your service desk provider — efficient support for mobile devices is an absolute must in today’s workplaces.
Third Big Challenge: Security

Financial services firms must insist on mobile devices, networks and practices that are secure and pose no new threats and risks to their organization. This is perhaps the biggest and most important challenge, given the sensitivity of financial information and transactions and legal implications involved in a breach.

Among the workplace security concerns with BYOD:

- Having a wide variety of mobile devices, operating systems, software versions and carriers, many of which are designed more for consumer use
- Employees less willing to accept restrictions on their own personal devices
- Multiple access points from different geographic locations and networks, from home networks to coffee shops, and mobile data connections with varying levels of security
- More opportunities for loss or theft of sensitive data
- The threat of large fines for compromised data in what is a highly regulated industry

Indeed, financial services’ IT staffs and resources will be put to the test to develop and enforce strong mobile security policies and mechanisms. But it can be done — and is an absolute necessity in today’s competitive marketplace.

Tips for Managing Security

1. Establish a policy governing use of mobile devices at your organization, including BYOD, that addresses:
   - Which devices and operating systems you will permit — iPad® and iPhone® but not Android, for example, or vice versa; make it clear
   - Required security features to use for each device, such as having passwords or lock screens, multi-factor authentication, data encryption and other security controls
   - Which applications will be required, allowed and/or banned — some proprietary apps may be mandatory for employee use, but apps for social media and personal email, for example, may present security or legal risks
   - Device monitoring and acceptable use provisions, such as what happens if an employee accesses an objectionable website on an iPhone® connected to a company VPN; also, how this would be enforced (set expectations)
   - What happens when employees leave the company — for example, can their devices, including personal information, be wiped?

2. Choose an enterprise mobility management partner that offers comprehensive provisioning services. With provisioning, a certificate is attached to identify each mobile device, enabling your IT department to determine if a device attempting to access the network is from an authorized user. Provisioning starts with an online portal (mentioned above) that gives end users a choice of their devices, carriers and plans. Once an order is placed, the partner can provision the choice with the proper policies and authentications.

3. Find a partner who can also help with a mobility risk assessment and mobility management. Supporting mobility and BYOD programs doesn’t mean your company must actively manage the devices or all the issues related to their use. You likely don’t have the resources or the budget for that. A better plan is to have a managed services provider you can trust to assess your risks and provide mobility management services, such as advice for improving security at endpoints and the potential for network and storage issues. The provider must be skilled at handling the types of mobile devices you choose to support.
Conclusion

Security issues, especially in a customer-focused industry such as financial services, make Bring Your Own Device and mobile adoption fraught with risk and challenges — as well as beneficial to employees and potentially a cost-saver to the organization. Enterprise mobility management solutions, as well as clear-cut policies and strong enforcement, help enable safe adoption and peace of mind. Plan well, and find a collaborative partner in your IT solutions provider.

Next Steps

Visit CompuCom’s Enterprise Mobility Solutions page. CompuCom can help you provide device and application choice for your tech-savvy financial services employees, while maintaining a level of security, compliance and cost control that mitigates company risk.