WHITE PAPER

Financial Services Optimizing BYOD Strategies for Success

Sponsored by: AT&T

Denise Lund Jerry Silva
October 2015

IDC OPINION

Adapting to the evolving mobile environment is a challenge for any organization. For today's financial services institutions, the challenge is often intensified due to data security and risk management requirements. Financial institutions are focused on building and maintaining competitiveness by improving the customer experience. This includes providing employees with access to financial data in a variety of settings, and in turn, this often means accessing sensitive financial institution and client data through either company-supplied devices or the employees' personally owned devices. Line-of-business executives are often frustrated by the limitations caused by the need to satisfy auditors and improve security while trying to increase transparency and responsiveness to the customer's needs.

The financial institution can, to some extent, dictate the use of corporate-approved devices to individuals as part of specific business functions, like wealth management financial advisors, and can thereby mitigate risk by controlling those environments. But as a result of the sizable and growing presence of employee-liable mobile devices, financial institutions must also embrace this bring-your-own-device (BYOD) world. Unfortunately, a majority of financial institutions are leaving themselves at risk when it comes to their mobile policies. According to a recent survey by IDC, two-thirds or more of financial institutions have yet to optimize and deploy enterprisewide mobile governance regarding mobile devices, mobile security, and mobile application access for employees across both organization-provided devices and employee-liable devices. This is according to IDC's 2015 *Mobile Enterprise Software Survey.*

For a financial institution, addressing the BYOD world necessitates first and foremost that management evaluate the end-to-end impact of BYOD on the organization, particularly in terms of security, privacy, compliance of applications, content, data access, and employees' mobile device usage policies. Just as important, financial institutions need to select a solution provider partner that has flexible, scalable solutions; a broad ecosystem of partners; and proven professional expertise across a range of mobility aspects, including network, services, security, and devices. AT&T, among other solution providers, is focused on these types of BYOD solution differentiators, placing the vendor in the consideration set of financial institutions.

Mobility in the workplace will not stand still and in fact can benefit a financial institution by leveraging the preferred means of contact by its staff. Planning for the current and future state of mobile network strategies and device, content, and application management solutions is crucial for BYOD to be a success. For financial institutions, the risk of data compromise, among other security risks, serves to increase the urgency for management to begin the process of embracing a robust, well-managed BYOD environment.

IN THIS WHITE PAPER

This IDC White Paper discusses the growing list of challenges that face financial institutions in increasingly BYOD environments. The paper also discusses the diverse solutions available to manage such challenges of BYOD environments, paying particular attention to solutions that can mitigate the financial, security, and operational risks involved. The paper concludes with IDC's recommendations for decision makers charged with managing BYOD environments.

SITUATION OVERVIEW

BYOD in Organizations Is a Growing Reality

Businesses of all types are finding themselves face to face with employee-owned devices that use a wireless network to access organizational data, content, and applications. In fact, over one-third (38%) of U.S. enterprises report that they have employees bringing in devices of their own choosing to use for work purposes, according to IDC's 2015 *U.S. Mobile Enterprise Services Survey*. On average, 54% of employees who have mobile phones – regardless of whether the employer or employee procured that device – use mobile applications other than email or messaging. As a result, the burden is on management to ensure that mobile access is secure, devices are managed, and policies for employee usage and reimbursement are in place. Enterprises of all types continue to have heightened interest in security and device management solutions.

Businesses face many risks due to adoption of a BYOD environment. Many BYOD devices do not yet have the software and services that allow management to implement and enforce access and usage policies. Further, reimbursement regulations in California have tipped in favor of the employee who must use a mobile phone for work calls. It is now the responsibility of the employer to bear the burden of financial reimbursement in such situations. The blurring of the line for financial responsibility between employee and employer is happening at warp speed, leading many organizations to formally address and implement new reimbursement policies. Just which BYOD mobility solutions are best for specific organizations varies by the unique challenges the organization faces; organizations in industries such the financial industry face a growing set of BYOD challenges stemming from a desire to provide anytime, anywhere service while maintaining security, privacy, and compliance. Given the sensitivity of financial data and the intensity of privacy requirements, in few industries are the security and compliance risks of BYOD more apparent – and expected to evolve continuously over time – than in financial services.

As with most mobility trends that organizations face, financial services management hopes that the benefits outweigh the challenges. As employees become increasingly mobilized, these institutions can expect to achieve improved customer experiences, cost savings from expanding their mobile workforce (particularly in areas like wealth management and lending), and the ability to attract and retain new staff from today's mobile-centric population as a growing number of employees in the financial services industry want to use their own mobile devices to access company networks and applications. For example, one of the biggest issues in financial services IT today is the hiring and retention of IT staff, where mobility has become so ingrained in the millennial lifestyle that these employees prefer using their own personal device over the corporate-liable device. Carrying multiple devices can be cumbersome. As the use of these employee-liable devices gains traction in financial services organizations, BYOD will create additional mobile security, policy, and risk management challenges. However, the potential benefits of BYOD can easily outweigh the risks in financial

institutions if management chooses partners that bring a breadth of on-target BYOD strategy, expertise, and solutions.

BYOD Challenges and Solutions

When it comes to BYOD, financial institutions typically face major challenges in four distinct areas:

- The regulatory environment (e.g., Gramm-Leach-Bliley [GLB] Act, Sarbanes-Oxley [SOX] Act, PATRIOT Act)
- Security of the device, as well as security and access to business and client content and applications
- Updates, policy changes, and support issues
- Financial implications of voice and data usage

Each challenge as well as ways to address the challenge in financial institutions is described in the sections that follow.

Financial Institutions and the Regulatory Environment

While the financial services industry is well known for its complexity, risk, and increasingly high requirement for information privacy, management must now contend with the addition of mobile devices. The access and disclosure of financial and personal information is highly regulated and failure to comply with regulations comes with potentially large fines. In addition, business payment data also needs to be secured and is regulated under other legislation (e.g., credit card information falls under the Payment Card Industry [PCI] Security Standards Council). Financial services employees who use their own mobile devices for work purposes put a spotlight on these regulations — regardless of whether or not their organization has a formal BYOD policy. Of particular concern are those regulations governing personal or proprietary content due to the potential for negative or unfair consequences should such content be compromised. Audits by organizations like the OCC, NAIC, and SEC can require the financial institution management to produce documentation on communication channels, forms, and network usage by employees using their own devices to access data belonging to their organization and its clients.

Addressing the Challenge

Solution providers run the gamut from providers that install security on the device or within the application itself to network-oriented security and providers that offer mobile life-cycle management (MLM) services. IDC defines mobile life-cycle management services as mobile device, connectivity, application, and security solutions that are offered by third parties to manage the efficiency and effectiveness of mobility in the organization. Mobile life-cycle management services include a variety of elements that are hosted either on or off customers' premises. Many of the managed elements leverage enterprise mobility management software that is licensed by the third-party service provider and/or resold to the customer as the foundation on which an organization wraps its mobile life-cycle management services. Solution providers, such as AT&T, sit at the nexus of these solutions, with proven experience in making the solutions come together by leveraging network services and devices. The solutions, whether deployed at the network level, device level, or user level, help organizations minimize the chance or degree of policy infractions and security risks.

Securing the Device, the Business Content, and Access to Business Applications

With the BYOD trend comes serious security implications. Malware from employee-liable devices that access the financial institution's network can compromise proprietary data. In addition, there are risks associated with the loss or theft of the mobile devices themselves. Such losses have put client and organization data at risk through unauthorized disclosure, with the organization itself facing the real possibility of litigation and stiff financial penalties.

In the financial services industry as well as in other industries, employee-liable devices challenge management to enforce security policies on devices that are not owned and managed by the IT department. These concerns intensified after the creation of the Consumer Financial Protection Bureau (CFPB) under Title X of the Dodd-Frank Act in 2010. Focused on protecting customers of the financial services industry in the United States, the CFPB has the authority to regulate and fine institutions and executives of those institutions for failure to maintain privacy and security of consumer data. In October 2014, the CFPB finalized new rules under GLB with regard to nonpublic personal information (NPI). This is just the start of the CFPB focus on ensuring that financial institutions comply with strict rules regarding the privacy of consumer information. At the end of the day, the BYOD trend raises the need for financial institution management to pursue an evaluation process — from the organization's network to its underlying infrastructure — for protecting applications, content, and data on mobile devices. To do this, organizations must establish policies and procedures for mobile security to ensure compliance among all the employees and their devices.

Addressing the Challenge

Organization decision makers are increasingly prioritizing secure mobile access among employees to corporate resources and content according to IDC's *U.S. Mobile Enterprise Services Survey.* Connectivity and policy management solutions help assure organizations that employees are able to access approved business content and applications while minimizing risks to the business. These solutions include a heavy emphasis on security processes and are not aimed at the device itself but rather what applications employees use via the mobile device. Services include, but are not limited to, distribution of applications, integration via APIs, email and personal information management (PIM), and content sharing management and policy enforcement. Management of applications, when not at the holistic device level, is either via a containerized approach or at the application level. In these situations, management can operate with added comfort knowing that BYOD employee devices can be prohibited from going outside the firewall to download applications from public application stores.

Even with solution providers such as AT&T available to help organizations implement private business application stores, employees may still find ways of using their own device to access applications via other channels outside of the organization's firewall. Mobile device management and mobile application management software are essential pieces of a holistic BYOD environment for banking, capital markets, and insurance. These services are provided by solution providers such as AT&T and enable organizations to more fully control devices and corporate information whether those devices are employer owned or BYOD.

AT&T Advanced Solutions offers a managed service to help enterprise clients address challenges and opportunities to drive business transformation through mobility. AT&T offers end-to-end solutions services in mobility consulting, BYOD, enterprise mobility management, device life-cycle services, mobility managed services, and network and technology transformation. Solutions such as these have been thoughtfully cultivated to accommodate organizations looking for technology that can grow with them as their needs evolve. AT&T allows management to pick and choose the most appropriate

capabilities that best meet their organization's specific needs. AT&T has a list of trusted providers including AirWatch by VMware, IBM MobileFirst Protect, MobileIron, and OpenPeak that bring unique strengths as part of its enterprise mobility management focus. AT&T's ecosystem brings together a range of solutions from those that take traditional mobile device management and security approaches to others that focus on containerization and PIM approaches. AT&T has also gone so far as to pre-integrate with security threat assessment vendors, such as FireEye and Blue Coat Systems.

End-user, or enterprise employee, 24 x 7 support services are often part of mobile life-cycle management services and very much a part of AT&T's offering. This type of solution provides the institution with efficiencies when addressing the many support-related questions that need to be fielded over the life of the device. By having 24 x 7 end-user support, organizations can focus on core competencies, without the need to hire internal staff who have the bandwidth and expertise required to provide end-user device support. Online support is basic, and phone support may be available.

Maintaining Updates and Policy Changes

Across a wide range of industries, mobile device usage in the workplace has evolved from a two-way communications tool into one that heavily utilizes organizational knowledge bases, applications, and other content that may sit behind a bank firewall or at a third-party location (i.e., cloud service). Financial services institutions are currently embarking on a massive move to digital transformation, updating technologies and processes, and expanding access to financial data. The stakes are therefore significant when it comes to customer privacy, whether consumer, small business, or corporate. Risk management and a focus on compliance often requires the help of a knowledgeable partner that has in-depth expertise in the types of risks that may crop up. Knowledgeable partners can help the organization conduct a mobility risk assessment, including defining mobile worker profiles to understand who needs access to what data, where, and how and on which devices to identify potential security risks.

There can be a mindset within IT that "we're going to save money with a BYOD strategy," but that isn't always the case if the strategy is not implemented properly. Indeed, organizations should determine up front how they will provide support to employees who use their own devices for work. Enterprise mobility is relatively limited at most financial institutions, so IT help desk support for business applications or FAQ-oriented, self-help options for these employees are limited as well. The impact of downtime among employees stands to wreak havoc on an organization's priorities — customer care, efficient and effective access to knowledge bases, records management, and productivity and customer experience all can be adversely affected. Support for employee-liable devices is a requirement for all organizations that want to embrace BYOD successfully, yet quantity and availability of knowledgeable IT support resources can be a challenge in some organizations.

Addressing the Challenge

For all these reasons, professional and consulting services are essential in the BYOD solution design, implementation, and life-cycle management phases. Providers with these capabilities can partner with a financial institution's management and IT teams to help the organization operate as a center of excellence. Even more importantly, these vendors can help an organization create and execute on an overall strategy to address BYOD risks while maximizing opportunities. Enterprise Mobility Management Services (EMMS) from AT&T, for example, provides services that are aimed at fulfilling this highly strategic partner role. The vision that the organization's executives and IT team has can be shaped by AT&T at the outset of the organization's relationship around BYOD solutions. Essentially, AT&T offers a mobility systems integration function within its EMMS team, offering three tiers of tech

support focused on the management and IT team's support needs (i.e., enterprise mobility management [EMM] configuration support) rather than end-user support. (That support is provided by a different team within AT&T.) AT&T then provides the follow-up phases of installation, configuration, training, and even full remote administration of the Enterprise Mobility Management platform. AT&T has multiple years of experience in risk mitigation strategy design services, systems integration functions, and related implementation and support.

From a mobility perspective, this is just the start. Financial institutions will need to scale their rollout of the BYOD strategy over time. The importance of consultation and workshops between the BYOD services provider and the business management and IT team is crucial. The openness of the strategic services vendor to this type of relationship is a key decision criterion that organizations should have in mind. The professional and consulting services teams that are worth their weight in gold are those that will help the organization discover hidden costs in one BYOD solution approach versus another, as well as recommend a phased approach to embracing BYOD in the organization.

Managing Financial Implications of Voice and Data Usage

Today's younger professionals, including employees in financial institutions, often prefer to use their own mobile devices rather devices provided by the organization. This has shown to be especially true of new IT professionals recruited by financial institutions today. Nonetheless, the expectation may exist that the financial institution will at a minimum compensate for the increased mobile plan usage. A court ruling by the California Court of Appeals (Cochran v. Schwan's Home Service) on BYOD mobile plan usage reimbursements firmly sided with the employee. The ruling essentially states that employers in the state must reimburse the voice usage in situations where employees are required to use their own device for work purposes. It is up to employers to deal with the complex task addressing the appropriate amount of BYOD usage in an efficient and effective manner. This will add incremental burden on the organization as it has to process either a stipend payout per employee, manage receipts and subsequent reimbursements per employee on a monthly basis, and even manage the process by which employees verify work-related usage. There are numerous inefficiencies in these sorts of manual processes that may end up costing the organization time and money that could be spent elsewhere.

Addressing the Challenge

Recent IDC research around digital transformation (DX) points to a critical aspect of transformation — the employees or WorkSource DX. More and more, financial institutions are responding to the demands of the current labor pool by appealing to the lifestyle of today's workers. And more often than not, this includes the flexibility for staff to shift hours and locations to better complement their schedules and home lives. The good news for the institution is that this creates a better chance of retaining the employee, as well as the potential of better productivity. However, this flexibility also means that the institution is faced with managing the separation of personal and business content on employee-liable devices and the need to preset voice and data spend limits on employee-liable phones in order to avoid unpredictable operating expense from this critical connectivity environment. Technologies like the AT&T Work data solution can be applied at the application level, helping management mitigate the risks posed by employees who use their devices while at work to access nonbusiness content. The solution can be integrated with trusted enterprise mobility management solutions providers, affording financial services institutions a choice of which solution provider will best meet the organization's needs. In addition, these solutions allow employee-owned devices to have a work phone number that is owned by the organization. This capability helps reduce compliance

challenges while also streamlining the reimbursement process — regardless of what mobile operator's network the employee-owned device is on.

FUTURE OUTLOOK

Mobilizing employees no longer means simply providing smartphones to executives and field service workers and enabling basic voice and data communications. Mobility in the enterprise is far beyond this stage, now involving provisioning and securing multiple device types (i.e., smartphones and tablets) for employees across a wide range of job functions. Increasingly, mobilization also means managing and monitoring devices brought by employees as part of the mix, which in turn involves monitoring and securing access to business applications and content. Complexity and cost implications have increased dramatically for enterprise IT departments in terms of managing the mobility life cycle. Optimizing the usage and cost of the services and enabling access have become massive tasks because of the proliferation of mobile devices in the enterprise. A recent IDC survey confirmed that 53% of U.S. enterprise employees are using smartphones in the workplace, up from 38% in 2013 (see *The Enterprise Is Fully Onboard with Mobility, Now Looks to Security and Services: Key Findings from the 2014 U.S. Mobile Enterprise Services Survey,* IDC #250570, August 2014). Acceptance of BYOD is commonplace in businesses globally today. However, IT administrators are struggling to balance the potential productivity and employee satisfaction benefits of BYOD with the security risks to networks and content. Ultimately, policy monitoring and management and security are as important to a successful BYOD strategy as are access to corporate applications and content. Many financial institutions have a mix of devices brought by employees and devices provided by the enterprise. Service providers such as AT&T recognize the need and have designed the modules of their mobility life-cycle management services with this in mind. The vast majority of service providers offer connectivity and policy management services that are able to handle devices brought in by employees in addition to corporate-provided devices. Container management and dual-persona software and services are targeted to BYOD environments.

CONCLUSION

The move toward BYOD environments is expected to grow and evolve over the next five years. Decision makers at financial institutions who are faced with BYOD have numerous considerations including how to provide network access, how to secure organization and client data accessed by these devices, how to facilitate device updates, and if and how to facilitate reimbursement to the employees who are using their own devices for work.

When it comes to BYOD, financial institutions cannot afford to operate without policies and governance procedures for employee-liable devices. According to IDC's 2015 *Mobile Enterprise Software Survey,* more than 50% of financial institutions report that their mobile deployments have been met with security and compliance issues. This is the highest incidence of reported challenges than in other major vertical industries.

Essential to financial institutions embracing BYOD successfully are the following management considerations:

- **Create a strategy to prioritize and leverage a range of BYOD approaches, including the impact of regulatory guidelines.** Such approaches should both protect and optimize the financial institution and its resources today and grow with an organization's future needs.

- **Discuss, evaluate, and assess options with a chosen strategic partner, such as AT&T.** Such discussions can and should be business oriented rather than technically focused, helping management take a leadership role in driving the organization successfully forward within a BYOD environment. Having confidence in the solution provider's ability to demonstrate deep technical supporting functionality behind the scenes is even more essential.
- **Engage solution providers in discussions and plans around goals for BYOD.** Consider the scope of BYOD functionality such as productivity, internal communication, and lines of business like lending and wealth management. Take into account the impact that mobilization will have on how the organization currently operates. Look for service providers that have the ability to apply financial services industry solutions when and where most appropriate.
- **Choose solution providers that offer a broad set of capabilities through an ecosystem of partners.** Solution providers, such as AT&T, as well as some systems integrators, focus on providing a diverse set of products and consultative services that can help yield financial benefit, security, regulatory compliance, and operational efficiency. AT&T has invested in a solution strategy that affords clients the opportunity to select from a broad set of solution and partner vendor expertise yet benefit from the proven expertise AT&T has in working with the enterprise.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com