Taking Your Enterprise Mobile: The Executive Checklist

Mobile opportunities

Even though the transition of mobile phones into computers has been a long time coming, the sea change in the past two years is dramatic: Consumer mobile devices are so compelling and offer business users such a powerful medium for learning, transacting, sharing, and presenting that companies are willing to upend the "way we do things around here" to have them.

Becoming a mobile enterprise means new opportunities for your organization. Employees are happier and more productive when they have mobile access to their email, apps and data on tablets and smartphones. Companies running their businesses on mobile workstyle solutions gain competitive advantages and drive top-line growth.

In a recent survey, Aberdeen found that best in class enterprises are three times as likely as all others to tie business workflow to users' mobile devices.[1] Yet, according to nearly every analyst study, security is the primary inhibitor to both enterprise mobility and "bring your own device" (BYOD) programs. CSO Magazine recently reported that 17 percent of enterprises have already experienced a mobile breach.[2]

And yet…

Here's the rub. The audit committee, C-Suite, and board alike agree—even as they gleefully tap-tap on their favorite devices—that letting employees choose their own devices and then access corporate resources, apps, and data is a risky proposition. Unlike standard-issue, locked-down PCs or tightly controlled Blackberry® devices, mobile devices in today's enterprise are diverse, have varying levels of vulnerability, and offer no consistent way for IT to manage even the most basic security like passcode enforcement.

With an increasing number of companies issuing sensitive business documents to their boards of directors via the Apple® iPad®, the consequences of data breach are more easily imagined. Still smarting from data breaches that put companies out of business in the mid-2000s and with skin in the game as a result of Sarbanes-Oxley, executives and board members have an urgent need for their organizations to govern and secure mobile devices.

Mobile security concerns

While mobile security concerns range from passcode enforcement to device encryption, data breach and data leakage are at the top of the list for implementers of mobile workstyle programs. According to enterprise security expert Jack Gold, organizations will lose three to four times as many smartphones as notebooks each year. Gold (rhetorically) asks us "with 32 or 64 GB of memory, how many records does a lost smartphone or tablet contain?"[3] At an estimated cost of more than $250 per lost record,[4] a data breach can be expensive. In fact, some research estimates the cost of a mobile breach at more than $400,000 for an enterprise and more than $100,000 for a small business,[5] and in some cases these costs can range into the millions.[6] This concern resonates as an increasing number of smartphones and tablets connect not only to the corporate network, but also access an increasing number of business applications and content repositories. Beyond data, enterprise IT and security departments are concerned about the risk of opening up the internal network to a diverse array of mobile devices. In many cases, mobile devices are neither governed nor monitored, meaning that they can introduce network threats and negatively impact an organization's compliance status.

There are three primary factors that contribute to enterprises' security concerns

1. With the Center for Telecom Environment Management Standards reporting that 78 percent of organizations allow employee-owned mobile devices in the business environment[7] and enterprise IT spending for Apple® iPad® tablets alone set to reach $16 billion in 2013,[8] mobile devices in the enterprise are not only skyrocketing in volume but are also expanding beyond the executive suites to rank and file employees. Further, whether mobile devices are corporate-issued or personally owned, the number of apps on those devices is increasing. Mobile analysis firm, Asymco reported an average of 60 apps per iOS® device.[9] Given that over half of organizations are supporting more than one device type,[10] the exposure of the corporate network to potentially non-compliant or malicious apps is immense.

2. People at all levels of the organization have a strong desire to arm the workforce with mobile devices and mobile access to corporate apps and data. Organizations are also mobilizing horizontally, across their lines of business. This can range from restaurant chains equipping hosts and kitchen staff with iPad tablets to airlines distributing the "flight bag" of electronic aircraft manuals, flight plans and compliance documents to its aircrews on their Samsung Galaxy Tabs. Such mobile access shows tremendous promise, but it also means that corporate data and network access will be in the hands of a larger number of users via an increasing number of devices, thus multiplying the risk.

3. While the security solution for enterprise mobility that we hear about most often centers on locking or wiping a lost or stolen device, the biggest threat is uncontrolled data sharing. With millions of users sharing data across an endless tapestry of cloud-connected endpoints, the potential for data leakage dwarfs that of the device loss/theft scenario. According to the Citrix Mobile Device Management Cloud Report, some of the most commonly deployed apps, such as Dropbox and Evernote, are also among the most frequently blacklisted by companies, which speaks to their simultaneous usefulness and business risk.[11]

These are just a few activities that can jeopardize sensitive data and expose the enterprise to mobile threats. The time is now for a secure mobile device management solution that offers real-time defenses at all layers of the mobile enterprise.

With Citrix, the audit committee can now breathe a sigh of relief

Mobile Solutions Bundle delivers the real-time defense enterprises need to capture the business opportunities that mobile business brings while safeguarding corporate IP, customer and employee data, non-public financial information, and business intelligence. With cloud-based and on-premise offerings, Citrix lets your IT professionals secure and manage the most comprehensive array of mobile devices, gain visibility into and control over mobile apps, and shield the corporate network from mobile threats.

Citrix Mobile Solutions Bundle offers your organization:

- **Enterprise MDM.** Give users device choice without impacting compliance needs.
- **Secure email, browser and data sharing apps.** Productivity apps that users love and IT embraces.
- **Mobile app containers.** Users get the apps they need and IT meets compliance requirements.
- **Unified app store.** Enable the business by allowing anywhere access to apps.
- **Identity management, single sign-on and scenario-based access control.** Manage user access and radically simplify the user experience.

Your role in your enterprise's mobile strategy

You're aware of the risks, and you know about Citrix and our secure mobile solutions bundle. You are now armed and dangerous so you can help your IT organization and the rest of your company embrace enterprise mobility and capture the many business opportunities it brings. Go forth and conquer.

Executive Checklist	
☑ Device considerations	• **Company goals:** Define your company's goals for enterprise mobility. Specify whether you are focused on productivity improvements, top-line opportunities, and/or employee device freedom. Ensure that your organization's mobile strategy reflects those goals. • **Device freedom vs. device consistency:** Ensure that your IT professionals have thought through device support tradeoffs between device freedom and choice or consistency and control. Make sure they (and you) are comfortable with the variations in device types and the governance and security the devices enable IT to have. • **BYOD vs. corporate-owned:** If you can't choose between 100% corporate-owned and "bring-your-own-device" program, determine if a hybrid scenario is more suitable for your company. For example, you can allow certain users to choose the device type (perhaps from a short list) while limiting the choice for other users to just one device. For example, a hospital can roll out a BYOD program for its permanent doctors and administrative staff, while deploying corporate-issued tablets that must remain on campus to its nurses.
☑ User considerations	• **Mobile enablement and eligibility:** Determine who will be mobile-enabled (executives? sales? hourly workers? Everyone?). If the answer is not everyone, decide which departments, title (i.e. managers and above), and/or business reasons qualifies to be mobile-enabled. Also, decide if this differs with users in the field or if they're not full time employees. • **Who pays for BYOD?:** Decide whether your organization will embrace a BYOD program, and determine whether your stance will be to tolerate, encourage, or even subsidize part or all of the device and/or wireless expenses. • **Number of devices per user:** Determine whether or not some or all users will be able to have multiple devices with an enterprise mobility solution. For example, can sales personnel enroll their tablet for demos in addition to enrolling their phone?
☑ App considerations	• **Which apps will you allow?:** Ensure that your IT department has thought through which mobile apps your organization will enable (just email, contacts, and calendar? business automation? ERP? custom applications?). Ensure that their app rollout plans makes sense for the needs and risk profile of your business. Make sure that the application access IT enables can vary by role, group, device, and whether the device is company-issued or personally-owned. • **How will you secure apps?:** Ensure that IT has the ability to restrict the mobile apps and resources, no matter what type of user or device path you choose. They should be able to secure any custom developed, third party or BYO mobile app, with comprehensive policy-based controls, including mobile DLP and other essentials such as the ability to remote lock, wipe and encrypt apps and data. • **Mobile business opportunities:** Get to know the mobile goals and timelines of your lines of business. Ensure that IT has taken into account whether your LOBs intend to mobilize their favorite apps for their users and partners, and whether they intend to develop or extend custom apps for specific devices.

☑ Data considerations	• **What are the rules around data?:** Review your IT organization's mobile data access policy to ensure that your organization can set role-, group-, device-, and even context-based policies for who will be allowed to access apps and data repositories containing intellectual property, personally-identifiable information, business intelligence, non-public financial data, future announcements, etc. Moreover, many users may have more than one device so make sure that users can securely access the same data in their apps, web, and data centers across multiple devices. • **Assess data risk:** Determine the value and risk of the data that employees will be accessing, and lay out the consequences of data loss or breach. Make sure you and your executive team/board are comfortable with the reward-risk tradeoff. • **Prevent data leakage:** Ensure that your IT organization can protect sensitive data. Make sure that your IT organization has planned for how it will prevent leakage of sensitive data via mobile devices. • **Facilitate collaboration:** Beyond data protection, make sure that those who need access to data can get to it and interact with it easily. Streamlining access will support your security policies because users will be less apt to try to work around the security measures you put in place.
☑ Policy considerations	• **Standards compliance:** Review the regulatory, industry, and corporate policies to which your organization is beholden (regulations like HIPAA, industry guidance such as PCI, guidelines such as from the SEC, IT frameworks such as ITIL, other corporate policies), and ensure that your mobile strategy supports your current compliance controls. • **Privacy and global considerations:** Review the foreign laws and regulations for regions in which your company operates or serves customers, and ensure that your mobile strategy supports your adherence to those policies. This includes not just security, but also user privacy regulations that may inform how you implement enterprise mobility solutions in the various locations in which you operate. Review your mobile device and access policies (policy setting, oversight, and reporting) with your audit committee, C-Suite, and board of directors. • **Employee mobile contract:** Set policies with clear considerations and limitations around device ownership, liability, replacement, support and monitoring. Beyond security and access policies, consider the mobile "contract" between the business and users. Who owns the device and pays for service? Who is responsible for device replacement? In addition to all of this, set a clear policy around device retirement upon employee departure. • **Minimum policy requirements:** Determine your flexibility level for the devices that will not enroll in a full mobile solutions bundle. For example, will you set policies so certain users like contractors and users in specific regions can still access their email and/or an essential secure app on their mobile devices without compromising user privacy? • **Reimbursements:** If you roll out a BYOD program, will you offer a stipend or reimbursement for the device and/or service? If so, how will you manage this and who qualifies for this program? Will you still be able to take advantage of volume discounts from service providers?

☑ Security considerations	• **Device, user and app compliance:** Understand how your IT organization will handle the presence of rogue devices, unauthorized users, and non-compliant mobile apps on the network. • **Data security:** Understand how your IT organization will secure corporate data from unauthorized access, inadvertent loss, and insider threats. • **Threat monitoring:** Understand how your IT organization will monitor your security infrastructure for security threats as well as network, app, and device performance. If you have a log maintenance policy for compliance and forensic purposes, ensure that they are equipped to collect, maintain, and protect those logs. • **Decommissioning:** Understand how your IT organization will remove data from devices upon device loss or theft or upon employee departure. If you intend to have personally-owned devices in the workplace, consider your plan for removing corporate data while leaving personal content intact. Ensure that you have a plan to clearly articulate policies and processes to all affected employees. • **SIEM integration:** Understand whether your IT organization will integrate your mobile device management system with a security information and event management or other system, and ensure that there is a plan in place to do so.
☑ Scalability and high-availability considerations	• **Uptime:** Ensure that your IT organization has articulated and can support an uptime service-level agreement, and whether it maps to your business requirements. • **Business growth:** Ensure that your mobile strategy takes growth into account and enables your IT organization to support all of the users you would like to mobilize today and over time. • **Scalability costs:** Ensure that your mobile strategy enables you to scale users in a cost-effective way, and that all associated hardware, software, and service costs are accounted for. • **Redundancy and fault tolerance:** Understand your mobile strategy's high-availability plan. If your strategy includes load balancing, server and data redundancy, and (if a cloud-based solution) global redundancy for disaster recovery, ensure these investments are in the plan.
☑ Service considerations	• **QoS considerations:** Understand whether your mobile strategy includes monitoring telecommunications service quality. If so, ensure that your IT organization can articulate what actions you will take as a result of the business intelligence you garner. • **Telecom expenses:** Understand whether your mobile strategy includes managing telecommunications expenses. Ensure that you have articulated your savings goals and measurement mechanisms for evaluating your progress against those goals. • **Remote support:** Understand whether your mobile strategy involves providing remote support, diagnostics, and troubleshooting, and what mechanisms are in place to do this. • **Employee self-service:** Understand whether your IT organization intends to offer a self-service portal for users to perform basic security and management actions on their devices.

About Citrix Mobile Solutions Bundle

The Citrix Mobile Solutions Bundle, which is comprised of XenMobile MDM and CloudGateway, is an enterprise mobility management solution that enables complete and secure mobile device, app and data freedom. Employees gain quick, single-click access to all their mobile, web, datacenter and Windows apps from a unified app store, including beautiful productivity apps that seamlessly integrate to offer a great user experience. The solution provides identity-based provisioning and control for all apps, data and devices, policy-based controls, such as restriction of application access to authorized users, automatic account de-provisioning for terminated employees and selective wipe of apps and data stored on lost, stolen or out-of-compliance devices. With the Mobile Solutions Bundle, IT can meet users' desire for device choice while preventing data leakage and protecting the internal network from mobile threats.

1. "Mobility in ERP 2011", Kevin Prouty, Aberdeen, May 2011
2. "Global State of Information Security Survey", CSO Magazine, 2012
3. "MDM is No Longer Enough", Citrix webinar with enterprise security expert, Jack Gold, October 2011
4. "U.S. Cost of a Data Breach", Ponemon Institute, March 2011
5. State of Mobility Survey, Symantec, February 2012
6. In 2010 the average cost of a data breach was $7.2 million. Doug Drinkwater, Feb. 10, 2012, TABTIMES.COM
7. marketwatch.com/story/ctemsr-research-78-of-enterprises-allow-bring-your-own-device-byod-2012-07-24?siteid=nbkh
8. "Global Tech Market Outlook for 2012 and 2013" Andrew Bartels, Forrester, January 6, 2012
9. "More Than 60 Apps Have Been Downloaded for Every iOS Device", Asymco, January 16, 2011
10. "Market Overview: On-Premises Mobile Device Management Solutions", Forrester, January 3, 2012
11. Citrix Mobile Device Management Cloud Report, Q3 2012

CITRIX®

About Citrix

Citrix (NASDAQ:CTXS) is the company transforming how people, businesses and IT work and collaborate in the cloud era. With market-leading cloud, collaboration, networking and virtualization technologies, Citrix powers mobile workstyles and cloud services, making complex enterprise IT simpler and more accessible for 260,000 enterprises. Citrix touches 75 percent of Internet users each day and partners with more than 10,000 companies in 100 countries. Annual revenue in 2011 was $2.21 billion. Learn more at www.citrix.com.