IBM Global Technology Services
Thought Leadership White Paper

November 2012

Developing more effective mobile enterprise programs

A practical "how-to" guide for creating mobile enterprise programs with help from partners

The proliferation of mobile devices, along with an increasingly global and remote workforce that demands instant access to corporate resources, has created a tremendous need for mobile enterprise programs. These programs encompass the infrastructure, technologies and policies that enable employees and other stakeholders to implement enterprise applications and access corporate resources on mobile devices—such as smartphones and tablets. Although some companies permit employees to work only on corporate-owned mobile devices, others are increasingly implementing "bring-your-own-device" (BYOD) programs, which allow employees to select and buy their own mobile devices for work functions.

Mobile enterprise programs can enable companies to create significant value for employees, partners and customers. With around-the-clock access to corporate resources, employees can work in virtually any location—and companies can enhance their overall productivity, efficiency and competitive edge. But mobile enterprise programs can also pose significant challenges for organizations. With few best practices firmly entrenched in the industry—due to the rapid and very recent growth of mobile technologies—many companies who want to create mobile enterprise programs do not know how or where to begin. Others who choose to develop their programs in house are finding it to be a time-consuming, costly, complicated and risky endeavor.

This paper outlines practical "how-to" guidance to strategize and implement more effective mobile enterprise programs and details the robust capabilities that mobile enterprise partners can bring to the development and support of your corporate-owned device or BYOD mobile enterprise programs. It focuses on mobile enterprise programs for employees, as opposed to customers.

The consumerization of IT

The widespread demand for mobile devices in the workplace, coupled with an increasingly dispersed workforce, has forced companies to support the usage of mobile technology in the workplace. In a recent IBM survey of 675 chief information officers (CIOs) and IT managers of large enterprises worldwide, 74 percent of respondents said they are placing greater priority on developing a flexible workplace compared to other investments over the next 12 months.[1] The majority of respondents also believe the flexible workplace will yield productivity gains, and nearly half believe it will potentially increase revenues.[2]

According to industry analyst Gartner, by 2014, 80 percent of mobile professionals will use at least two mobile devices to access corporate systems and data, up from 40 percent today.[3] It is clear that the use of mobile devices in the workplace is no longer a trend—it is a new corporate reality.

> *"The rise of 'bring your own device' (BYOD) programs is the single most radical shift in the economics of client computing for business since PCs[4] invaded the workplace. Every business needs a clearly articulated position on BYOD, even if it chooses not to allow for it."[5]*

Mobile challenges for enterprises

Because mobile technology is new and ever changing, few best practices have been established to give companies roadmaps for implementing effective mobile strategies. As a result, many enterprises do not know how or where to begin.

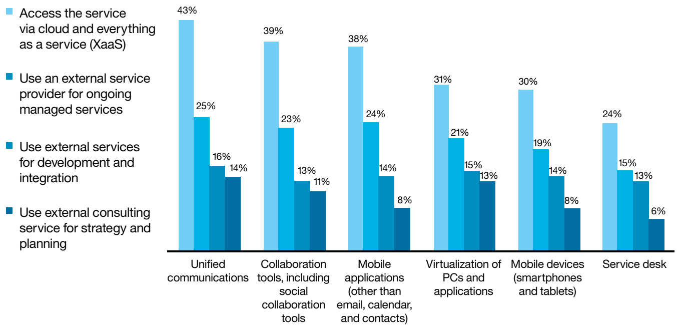
Security, privacy and usage governance are also major concerns—due to the intermingling of personal and corporate data on many mobile devices. In fact, 71 percent of chief executive officers (CEOs) and IT managers surveyed indicated that security was their most significant mobile enterprise challenge.[6]

And their concerns are not unwarranted. In its seventh annual study sponsored by Symantec, Ponemon Institute reported that the average organizational cost of a data breach is US$5.5 million and US$194 per record.[7]

The study also indicated that 39 percent of organizations had a data breach as a result of an employee or contractor's lost or stolen mobile device—which included laptops, smartphones, tablets and USB drives that contained confidential and sensitive information. In addition, 37 percent concerned a malicious or criminal attack, and 24 percent involved system glitches including a combination of both IT and business-process failures.[8]

Organizations cannot afford the potentially disastrous consequences of blindly navigating the rapidly evolving mobility maze. That is why many companies are increasingly seeking help from highly skilled professionals who can provide the resources and technologies required to help organizations mitigate risks and implement sustainable mobile enterprise programs. A mobile enterprise partner can also offer knowledge of best practices gained from helping diverse companies, across numerous industries, create successful mobile enterprise strategies.

How are you planning to implement your mobility, collaboration, and social business strategy and address related challenges?



Base: 80 global IT decision makers
Source: A commissioned study by Forrester Consulting on behalf of IBM, May 2012

"How-to" guidance for mobile enterprise development, management and support

There are four steps to implementing an effective and sustainable mobile enterprise program:

1. **Define a mobile strategy:** clarify your mobile goals, determine what type of program you will support (BYOD versus corporate-owned device) and evaluate cost considerations

2. **Implement your mobile enterprise program:** determine which tools you will use to build your mobile enterprise program and prepare your enterprise network to support your program

3. **Secure and manage your mobile devices:** choose technologies to help secure the mobile devices connected to your network and develop a mobile security policy

4. **Support:** provide ongoing break-fix support for mobile devices

Each stage is described in greater detail below.

Step one: mobile strategy development

One of the most critical steps to creating a mobile enterprise program should be to define a mobile strategy that will govern how you choose to develop and implement mobility in your workplace. Such a strategy should begin with clear thinking about your needs, desires and goals.

Questions you will need to answer include:

- Why do we want to implement a mobile enterprise program? What is our ultimate vision? What benefits do we hope to realize?

- What are the cost considerations of a mobile enterprise program? Do the costs outweigh the benefits for our situation?
- Will we own or require employees to purchase and use their own mobile devices? How much, if any, reimbursement will we provide?
- Do we plan to develop custom mobile applications, outsource the development of mobile applications or purchase prepackaged mobile applications?

Benefits of mobile enterprise programs: There are a plethora of benefits to mobile enterprise programs, but the most common include:

- Increased employee satisfaction—Employees enjoy working from mobile devices, especially devices and platforms of their choice. They also enjoy the flexibility of working from nearly any location and at their convenience.
- Easier employee recruitment and retention—Employees tend to prefer to work for companies that support mobile technology in the workplace.
- Enhanced productivity—By enabling employees to work virtually anytime and anywhere, they can accomplish more inside and outside of the office. In addition, the development of customized mobile applications helps employees do business in newer and more innovative ways.
- Improved customer relationships—Specialized mobile applications (apps) can enable companies to sell their products via mobile devices and provide their sales staff with near-real-time customer data. These robust capabilities can help companies monitor "the pulse" of a customer, respond to their needs and desires faster and provide better customer service.

General cost considerations: The cost savings that companies have reported vary widely. Factors can include investments in software, infrastructure (including the mobile devices themselves, if you choose a corporate-owned device approach), staffing or related support services, application development and even potential network upgrades. You will also want to consider less obvious costs such as software licensing fees, company reimbursement for mobile devices, international usage fees, taxation, insurance and miscellaneous soft costs. But of course, many of the benefits of mobile enterprise programs—such as increased productivity, workplace innovation, time savings and employee satisfaction—are immeasurable. And companies that out-task mobile enterprise services often experience significant savings.

CIOs reported 20 percent productivity gains and cost savings when they outsourced flexible workplace services.[9]

BYOD versus corporate-owned devices: Mobile enterprise program costs are also linked to the type of program you implement.

For example, BYOD programs can be more costly and complex due to the intermingling of corporate and private data on mobile devices and the more complicated measures required to keep personal devices secure. According to the Aberdeen Group, a company with 1,000 BYOD mobile devices will spend an average of US$170,000 more per year than the organization with a centrally procured, corporate-liable policy. The incremental and difficult-to-track BYOD costs include:

- Disaggregation of carrier billing
- Increased expense reports filed for employee reimbursement
- Added burden on IT to manage and secure corporate data on employee devices
- Increased workload on other operational groups not normally tasked with mobility support
- Increased complexity of the resulting mobile landscape with consequential rising support costs[10]

Control and ease of management is another factor to consider. If you select, own and manage mobile devices, it can be easier to secure them and to manage compliance with corporate policies—because you can create the infrastructure upon which you deliver corporate data and applications. But control may come at the expense of user satisfaction—because many employees adamantly prefer to work with their own devices. To facilitate widespread support of your corporate-owned device approach, get input from your employees regarding the types of devices and applications they would like to use. They are more likely to accept the limitations of a program they helped to build. In addition, if you are supplying the mobile devices, your employees will expect your organization to provide a high level of end-user support. Therefore, you will need adequate staffing and in-house expertise to support these new demands.

Strategy considerations—how a mobile enterprise partner can help: A mobile enterprise partner helps assess how mobility can benefit your employees, customers and business overall. They can provide strategy and consulting to help you clarify and prioritize your needs and goals, evaluate your tangible and intangible return on investment and develop a phased roadmap for program implementation. They can even offer telecom expense management services to help you optimize and better manage your mobile spending. And a partner can virtually eliminate the painstaking research and logistical challenges entailed in starting from scratch—to help you get your program up and running faster.

Step two: mobile program implementation

Once you clarify your program goals, you need to begin assessing how to technically implement them.

Questions you will need to answer include:

- What devices will we support (phones, tablets, laptops)? What are the advantages and disadvantages of supporting different devices and operating systems? Based on this analysis and end-user preferences, what devices and mobile operating systems do we want to support?
- What data and applications should we make accessible to end users, and should we grant full or restricted access?
- What services will we support?
- Who are the employees and stakeholders who have the highest-priority mobility needs? Should we limit mobile enterprise adoption to these individuals or extend access to all employees?
- What mobile device usage scenarios might warrant the development of special mobile applications?

- Should we limit our mobile enterprise program to strategic corporate locations or launch an enterprisewide program that can support multiple sites worldwide?
- To what extent do our enterprise and mobile systems need to be integrated?
- How can we support the optimal performance of our networks to facilitate the success of our mobile enterprise program?

Determining which devices to support: It is nearly impossible to securely and logistically support every new tablet and smartphone that comes to market. A more effective approach is to support specific devices and operating systems and to define these devices (as well as your explanation for why you will support them) in your mobile policy—a topic we will cover later in this paper. Ideally, your decision should be based on the current and intended uses of mobile devices at your enterprise, and an awareness of your employees' preferences.

But in general, supporting more platforms means more complexity. So one of the easiest ways to reduce complexity is to limit the number of devices and platforms you support. But it is also imperative to consider the advantages and disadvantage of various platforms, such as Research in Motion (RIM) BlackBerry, Apple iOS, Android and Windows. And when considering the advantages, prioritize what is most and least acceptable to your organization from a security standpoint. Many businesses support the use of BlackBerry phones because of their security-rich design. And although iOS and Android platforms can support higher levels of security, older versions of Microsoft Windows and Android may not. To help ease security, app compatibility and your service-desk burdens, it is a good practice to limit the number of operating system (OS) platforms and versions. And as your program and security infrastructure evolve over time, you can slowly expand your device and platform support.

Choosing data and applications for mobile access: Once you have narrowed down the devices and operating systems you will support, the next step is to determine the data and applications you will make accessible to specific employees. For example, if you work in a health-care setting, you may require different levels of mobile accessibility for nurses and doctors than for administrators. We recommend compiling a team that is charged with gathering information from your employees to gain more insight into their real and perceived needs for mobile technology in the workplace. This information helps you to more effectively brainstorm specific business processes—across your enterprise—that could be facilitated via access to specific data and existing or custom applications on mobile devices. Then, to reduce complexity, prioritize which users will have mobile access to these corporate resources. And be sure to "test the waters" first by extending access only to your higher-priority users as opposed to all employees.

Generally, to get started, email and calendar applications are more common and easier applications. If your employees are already using mobile devices to access their email and calendar, it is wise to take inventory of the devices and platforms they are using to help manage security compliance prior to updating or expanding your mobile enterprise program. If you are starting a BYOD program, realize that mobile messaging middleware has limited functionality (see "Device wipe and lockdown" on pages 8-9).

Enabling employee services: In addition to enabling applications, you may also choose to enable certain services through mobile devices. These may include social-business functions, such as instant messaging; enterprise-risk management (ERM); and customer-relationship management (CRM) systems for access to sales, financial and human resources (HR) data.

Prioritize the order in which you will make such services accessible to employees—because once mobile technologies are supported within your workplace, your employees will come looking for numerous capabilities.

Preparing your network: Efficient network management is often overlooked when planning mobile enterprise programs, but it can make all the difference to the success or failure of your mobile initiatives. In general, an expanding network that supports growing numbers of devices and huge volumes of data will demand increased bandwidth and strong capabilities for network oversight. That means you will need solutions that can automate configuration changes, analyze performance, manage security, provide a host of other management functions and support massive scalability (such as cloud-based or virtualized network tools).

Uptime also becomes a greater concern. As networks grow, the chance of error and security risks also increases. And these increased risks make capabilities for reliable and effective event management, root-cause analysis, change and configuration management, performance reporting and endpoint management all the more necessary.

A manageable phased approach for mobile strategy implementation

When developing a mobile enterprise program, avoid the temptation to do everything at once—even if you are working with a mobile enterprise partner. Keep a broader vision in mind, while taking small steps toward your goals. This way, you can manage and resolve problems you may run into along the way before you move on to more complex initiatives.

Here is a sample rollout for a mobile enterprise program, which you may implement over a course of several months or longer.

1. Manage existing devices accessing your email, calendar and other mobile applications: Using infrastructure management tools or mobile device management (MDM) software, take an inventory of the number of mobile devices assessing your network. And pay careful attention to how they are accessing your network (such as through a virtual private network [VPN] or Wi-Fi) and what data and applications are accessible on these devices. If possible, you should also determine the security status of these devices, including authentication procedures and application security. If you cannot access this information due to lack of MDM and reporting tools in place, you may want to set a deadline to suspend current mobile access usage and announce newer, more stringent policies and procedures for your employees when you have the technical capabilities to enforce them.

2. Expand managed access to all employees: At a minimum, most of your employees will want access to corporate email and calendar applications. Expanding these capabilities to all employees helps not only enhance satisfaction, but it can also give you a better glimpse into the logistics of implementing an enterprisewide mobile endeavor. This insight can determine whether to enable companywide mobile access for other data and applications.

3. Secure on-device content storage and synchronization: You can allow data storage over the network only—to help avoid storing local copies on devices, which would be a risk if they were ever lost or stolen. You could choose methods such as encryption and containerization to better secure stored content.

4. Inventory and prioritize commercial off-the-shelf (COTS) mobile apps available for existing software used by the organization: This helps provide the capabilities your employees need to be more productive with mobile access.

5. Develop or contract out custom apps as needed: Consider what services and processes may require the development of customized applications, and develop them based on your mobile priorities.

6. Deploy mobile applications when your security infrastructure is in order: The corporate applications that are enabled for mobile access should at least match the security of applications that are not enabled for mobile access. If you cannot deploy applications that pass this security standard, limit your deployment to more trusted mobile applications.

Step three: security management

After you have determined the technology you will use to build and manage your mobile enterprise program, you then need a plan to help secure all the mobile devices connected to your network.

Questions you will need to answer include:

- How can we better manage the security of devices, applications and data access?
- How do we manage data when an employee leaves the company or when a device is lost or stolen?
- How do we better protect the mobile devices from common threats, such as viruses, malware and attack?
- What is the minimum level of security that we will deem acceptable, and can we implement it given the confines of our corporate culture?
- How can we more securely distribute mobile devices and corporate applications and manage the onboarding and adoption process?
- What should be included in a mobile security policy, and how can we better manage compliance with data privacy laws?

Although mobile security remains a top concern for organizations, there are numerous ways to protect data on mobile devices. If you have already determined the mobile devices your organization will support and the minimum level of security that you will require, choosing the right tools to more securely support your mobile enterprise can be much easier.

There is a wide range of resources and security methods to choose from, some of which include:

Mobile device management (MDM): This represents the traditional IT approach of monitoring a device through a software agent that is installed on the device and a server that is either operated in house or via cloud-based services. MDM is useful for virtually any device that needs to be reported or verified. In addition, it can help you deploy, manage and even distribute corporate applications over the air (OTA) throughout your enterprise. MDM can even let you see what applications users have installed, prohibit access to restricted applications and suggest new applications or updates. Some tools also include a variety of self-service user portals that allow employees to reset their passcode, lock their device, and partially or fully wipe their device remotely if it is lost or stolen. Implementing MDM in house can result in costly capital expenditures. But software as a service (SaaS) cloud-based systems are faster to set up, easier to update and more cost-effective.

However, when configuring your MDM solution, consider what your corporate culture will allow, especially for personal devices. You may, for example, be able to put an agent on an Android phone that can do detailed software inventory, disable the camera, trace the global positioning system (GPS) location, and do partial or full wipes of the phone. But will your corporate culture support these capabilities or deem them too invasive?

Containerization: Some MDM programs incorporate containerization capabilities that use encryption and other methods, to create a barrier between corporate and personal data on mobile devices—making them appropriate and effective for BYOD programs. Although some organizations may choose to combine MDM and containerization for cost-savings and vendor management reasons, we have found that keeping containerization methods separate from MDM can significantly reduce complexity.

Device wipe and lockdown: One of the biggest challenges of securing mobile devices is the mobile nature of the devices themselves. Their portable size makes them easy to lose, and their mobile use necessitates tracking and management mechanisms to protect sensitive corporate data.

Wiping or deleting all data from the mobile device after a certain number of invalid password attempts can help reduce the risk of a brute-force attack. In addition, a "local wipe" initiated by an end user or administrator is a recommended practice when a device is lost or stolen or when an employee leaves your company or moves to a different position within your company. Locking a device after inactivity timeouts can also help reduce security risks.

If you are just starting a BYOD program and do not wish to install an MDM agent on personally owned devices, you should consider that mobile messaging middleware does not enable partial wipe or data separation.

Encryption and data-storage alternatives: Encrypting the data on mobile devices can provide an additional level of security. Hardware-based encryption, one of the most common methods, offers an advantage over software encryption because it is built into the device and may enhance performance. Browser and virtualized applications can provide alternatives to storing data on mobile devices. Little, if any, data is actually stored on the device; instead, data is requested and displayed as needed, reducing the risk of data loss. However, network access is required, so users cannot access data when offline or disconnected. In addition, performance may be less than that of a native-rich client accessing local data on the mobile device or end-user response time may be longer.

User-based authentication and fraud prevention: Two-step, user-based authentication—for logging onto the device and then onto the corporate network—can be set as the bare minimum requirement to help control and monitor who is accessing your corporate data and applications.

A standard numeric or alphanumeric passcode can be required to log into the device, and a more advanced authentication method—such as a smart card, digital certificate or token—can be used to access the network.

Although some devices only support passcodes, BlackBerry also supports smart cards. But advanced security measures can be integrated into mobile applications. For example, you can require additional authentication procedures for accessing especially sensitive data and applications. These may include biometric indicators, such as voiceprint, that you can verify against your records. A multilayered authentication method is an effective way to reduce security breaches.

In addition, if you plan to allow virtual private network (VPN) access to your corporate intranet, then include the capability to help control what Internet protocol (IP) addresses can be accessed.

However, all of these methods can be costly and complex to implement. Therefore, it is important to balance cost and ease of management when deciding which authentication and fraud-prevention methods to deploy.

Mobile threat management: Virtually all mobile devices can become infected with malware. But an effective approach to mitigating malware is to implement protective measures that are similar to the desktop and laptop environment. This entails requiring all customers to install and automatically run anti-malware software and conduct regular real-time scans.

You will need to proactively advise your employees to only download and install trusted applications and to take appropriate actions, such as virus scans, when suspicious applications are identified. Creating a custom app store that allows your employees to download only officially vetted and supported corporate and non-corporate applications can limit malware on your network as well.

Mobile security policy: Finally, you will need to create and enforce policies to help protect your organization from liability and security threats. Mobile security policies should be constructed with guidance from both your company attorneys and the IT staff or mobile enterprise partners who know the technical details of your mobile security measures. The key points of your mobile security policy should include:

- The mobile devices you will be supporting—including company-owned and personal devices, the level of end-user support you will provide and how to access support. You may also want to explain why you support specific platforms over others. For example, you may choose to only support platforms that enable encryption, which will rule out certain devices.
- Definitions of all key terms, including basic terms, such as mobile device and mobile device management.
- Who will have access to specific data and applications?
- The data and activities that your enterprise will monitor and track, differentiating between corporate-owned and personal devices. This may include texting, email, browsing the Internet, downloads, GPS tracking, instant messaging, storage of multimedia files and more.
- A privacy policy that details what you will and will not do with the information that is monitored and tracked on both company and employee-owned devices.
- The specific actions your company will take if the end user violates company-usage policies.
- Defined defensive measures, such as remote wipes, that the company will take if the device is lost or stolen, or if the employee moves to another position within the company or is terminated.

The agreement should be signed by both supervisors and employees. Once you develop your official mobile security policy, be sure to announce it to your entire organization and distribute updates to your policy as you change it. And publicize your mobile security policy in newsletters, corporate social networks and your intranet.

Mobile security policy style guidelines from Gartner[11]

- Keep the policy document short, ideally no more than a few pages.
- Be careful to use directive words appropriately, such as “must,” “should” and “may.” Standards provide instructions that must be followed. Guidelines provide suggestions that should be considered. Check that questions and decision criteria show when a standard or guideline may or may not be applicable.
- Put detailed process discussions and tutorial explanations in appendices or external documents, rather than clutter the body of the document.
- Never duplicate material that belongs in another document, especially involving documents under someone else’s control. Provide clear citations to external documents. Establish a line of communication with all such document owners.
- Avoid ambiguous conditional statements, such as “always this way, except when that way,” and statements based on nested negative tests, such as “if not this way, then not that way.” Lead with positive conditions that are clearly qualified.
- Make absolute statements (“always”) only when the condition is truly absolute.
- Expand acronyms only once, on first use.
- Provide a glossary of terms, including a repetition of acronyms, as the last entry at the end of the document.

Do not forget end-user satisfaction: When defining security policies, be mindful of the quality of the user experience. For example, requiring different applications for mobile versus desktop devices can limit the success of your program. Lockdown features for applications may also reduce your program’s popularity. In addition, employees expect automatic notification alerts when their device is not in compliance and guidance to self remediate. Be sure to give them such guidance by regularly communicating your security-compliance policies.

Step four: day-to-day support

You will need to manage security for your mobile devices on a regular basis and provide support to your end users.

Questions you will need to answer include:

- What level of management and support can we provide to corporate or personally owned devices?
- Do we have adequate in-house resources for implementation and support, or should we seek outside help?

Staffing for support: MDM tools and security management software can help you track and monitor mobile device activity on your network. But you will need the staff to support these capabilities and help continuously guard your network against threats from mobile technologies.

Your mobile enterprise program should also provide some level of support to end users. Upon launching a mobile enterprise program, the device-to-employee volume ratio can spike significantly, so you will need the staffing and the budget to support these new demands. And your staff will need deep mobile technology expertise to manage new support requests from end-users.

Support-delivery approaches: You will need to design an approach model to govern how you will deliver support. Some organizations will designate a specified period of time—typically a half hour to an hour—to work on a mobile device issue. Others may choose to provide support for only network issues as opposed to mobile devices themselves. Some companies even design mailing lists, web portals and wikis that encourage end-users to share their experiences about support issues. For instance, a user can post a question about configuring Microsoft ActiveSync on their device that other employees can answer. Another option is to require end users to buy insurance that covers support and replacement for lost or damaged devices, in which case, your mobile policy should define acceptable insurance providers as well as stipends for insurance.

Implementation, security and support—how a mobile enterprise partner can help: Mobile enterprise partners can provide you with the skills, technologies, training and support required to implement and manage mobile enterprise programs faster and more cost effectively than in-house solutions. Both point and end-to-end solutions may include:

- Mobile device procurement, staging and configuration
- Mobile strategy development
- Mobile device management and application development
- Hosted and on-premise security management
- Mobile policy development
- End-user help desk support
- Network optimization, reporting, monitoring and integration services
- Compliance tracking and enforcement
- Maintenance and depot services
- Managed mobile enterprise solutions that are designed to provide end-to-end strategy, implementation and day-to-day support

IBM mobile solutions and capabilities

IBM Mobile Enterprise Services for managed mobility

IBM Mobile Enterprise Services for managed mobility is designed to provide advanced MDM, strategy and support to a range of devices and operating systems that includes RIM BlackBerry, Apple iOS and Google Android smartphones and tablets, as well as many Microsoft Windows mobile-based ruggedized devices. We can procure, install, configure, run and manage devices across multiple platforms. And we offer a more flexible subscription-based pricing model that is built around your devices' requirements, usage needs and service options.

Our strategy services help you assess your business and IT environment for mobile readiness and design a plan for mobile device management. Key among the recommendations we may make are enterprise-strength security policies and governance structures that help manage compliance issues both inside and outside the organization. Our mobility infrastructure strategy and planning capability can help you make appropriate choices based on your user profiles and business needs.

IBM Integrated Communications Services

Integrated communications services focus on designing, implementing and managing your communications and networking environments to help optimize them for virtually "anytime, anywhere" unified business communications. These solutions are designed to enable you to support key networking environments and build differentiating advantage through business innovation.

IBM Telecom Expense Management Services

Telecom expense management (TEM) services can help you more quickly gain visibility into your communications spend patterns and identify areas for short-term and long-term savings through consulting, software and management services.

IBM Mobile Foundation

The IBM Mobile Foundation offering is designed to bring together key mobile capabilities into a single integrated package and help you address the full array of challenges and opportunities that the mobile channel presents. IBM Mobile Foundation delivers a range of application development, connectivity and management capabilities that support a wide variety of mobile devices and mobile app types.

The IBM Mobile Foundation offering includes the following products (which can be purchased as stand-alone products):

- IBM Worklight® to help you build, run and manage cross-platform mobile apps
- IBM WebSphere® Cast Iron® Hypervisor Edition to help you connect mobile apps to cloud and back-end systems
- IBM Endpoint Manager for Mobile Devices to help you control and manage end-user devices

IBM Mobile Foundation is available in two configurations:

- Enterprise Edition—A business-to-enterprise (B2E) package, with Worklight, WebSphere Cast Iron Hypervisor Edition, and Endpoint Manager for Mobile Devices, that is used by enterprises to manage internal apps
- Consumer Edition—A business-to-consumer (B2C) package, with Worklight and WebSphere Cast Iron Hypervisor Edition, that is used for commercial and customer-facing apps

IBM Sametime

IBM Sametime® is an industry-leading software that can deliver simpler and more seamless access to enterprise instant messaging, real presence, online meetings, telephony, video conferencing and more—wherever people are working. Sametime software can provide a more immediate and cost-effective way to help improve customer engagement and to help teams make faster, expertise-based decisions with people inside and outside of your business without travel costs.

IBM Connections

IBM Connections incorporates sophisticated analytics capabilities, near-real-time data monitoring, and faster collaborative networks both inside and outside the organization. These capabilities can be accessible on premises, in the IBM SmartCloud™ or by using a broad range of mobile devices. It integrates activity streams, calendaring, wikis, blogs, email capability, and more, and flags relevant data for action. It also allows for instant collaboration with one click and the ability to build social, more security-rich communities both inside and outside the organization to help increase customer loyalty and speed business results.

IBM Mobile Security

IBM Mobile Security can help you thwart malware, provide security-rich connectivity, offer more secure access to enterprise data and systems and build safer applications and a more reliable mobile app platform.
Our key security products include integrated, one-view dashboards and functionality to help better secure virtually any type of endpoint or network, whether a smartphone, a PC, a server or a router. We offer:

- IBM Security Access Manager—to help you simplify password management, strengthen access security and better manage compliance demonstration
- Enterprise Wireless Networks—security-rich and robust wireless network solutions that can deliver virtually “anytime, anywhere” communications

- WebSphere DataPower® Service Gateway XG45 appliance—to enable more security-rich web services, applications and data with customizable, scalable and automated service visibility and governance
- Hosted Mobile Device Security Management—to help protect your mobile devices against malware and other threats, providing the knowledge, technology and ongoing management that can make mobile device security virtually "turnkey"
- IBM AppScan®—to provide application security testing and risk management solutions
- IBM Lotus® Mobile Connect—to offer more security-rich connections from popular mobile devices to enterprise-hosted solutions

Why IBM?

For more than 15 years, IBM has been providing mobility solutions for hundreds of clients, and managing hundreds of thousands of mobile devices worldwide. Through IBM, you can access a wide range of services and innovative solutions that cover the entire lifecycle of the mobile environment—from mobile strategy development and implementation to security management and day-to-day support. You can also use our robust global infrastructure, which includes more than 5,000 integrated communications and networking professionals, 70 workplace-services call centers worldwide, 9 security operations centers, 12 mobility delivery and support centers and over 30 research labs supporting mobility.[12] And as an industry leader, we can help you reduce complexity by providing the capability to support nearly all your IT needs and virtually eliminate the challenges of multivendor service delivery.

IBM supports employee choice in mobile devices

More than half of IBM's global employee population is mobile. The company needed to expand its corporate mobility program—launched in 2004 with a single corporate-issued device—to accommodate a variety of new mobile platforms entering the workplace. Over the course of three years, IBM piloted mobile access with different devices and operating systems, adding new entries like tablets as the market produced them. IBM collaboration software became an integral part of the solution. By 2011, wide-scale production deployment was underway, with mobility viewed as a core infrastructure service. Today, the program covers 120,000 mobile users, including 80,000 personally owned devices, and continues to expand.[13]

> *"IBM's BYOD program really is about supporting employees in the way they want to work. They will find the most appropriate tool to get their job done. I want to make sure I can enable them to do that, but in a way that safeguards the integrity of our business."*
>
> —IBM CIO Jeanette Horan

Notes

For more information

To learn more about IBM products and services for mobile enterprise programs, please contact your IBM representative.

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

IBM Corporation
International Business Machines Corporation
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
November 2012

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

[1] IBM: "Achieving success with a flexible workplace," May 2012.

[2] Ibid.

[3] Gartner, "Seven Steps to Planning and Developing a Superior Mobile Device Policy," October 5, 2011.

[4] Personal computers.

[5] Gartner, "Gartner Says Bring Your Own Device Programs Herald the Most Radical Shift in Enterprise Client Computing Since the Introduction of the PC," August 29, 2012.

[6] IBM, "Achieving success with a flexible workplace," May 2012.

[7] Ponemon Institute," 2011 Cost of Data Breach Study: United States," March 2011.

[8] Ibid.

[9] IBM, "Achieving success with a flexible workplace," May 2012.

[10] Aberdeen Group, "Hidden Costs, Unseen Value," August 17, 2012.

[11] Gartner, "Seven Steps to Planning and Developing a Superior Mobile Device Policy," October 5, 2011.

[12] Statistics are current as of November 2012.

[13] Statistics are current as of 2012.