The typical employee uses three mobile devices for work. And there has been a large increase in the number and type of applications used on these devices, such as mobile collaboration, conferencing and social media. How is this changing the modern workforce?

Mobility is now ranked as the second highest technology priority among chief information officers (CIOs), and likely to become the top priority this year, according to Gartner data. This eBook looks at how IT departments can better support employees who are choosing where, when and how they want to work, while keeping corporate assets secure.

In the next three to four years, mobile internet traffic will surpass desktop internet traffic, driven by mobile data-enabled devices. Mobile devices, applications and services are dramatically reshaping enterprise revenue models, business strategies and how employees interact with other employees, partners and customers. As tablets and smartphone become ubiquitous in the enterprise, firms are looking to take advantage of these devices to improve the way they do business. Not only do they improve employee satisfaction and productivity, they also introduce greater efficiency into business processes, improved customer responsiveness, increased level of collaboration, and faster decision making. The key to enjoy those benefits is to develop a strategy for their introduction and management.

A central feature of enterprise mobility is the bring-your-own-device (BYOD) trend. Chief information officers and IT departments face a myriad of challenges when allowing employees to bring their own mobile devices into the work environment. Issues related to management, support, security and the ability to control access to corporate networks and assets abound. The BYOD challenges to enterprises are multifold, from overwhelming IT resources to losing valuable data and infecting corporate networks.

While some IT managers are looking at BYOD as an overwhelming challenge, others are looking at it as an opportunity to improve productivity and efficiency as well as replace legacy IT systems. Add to the mobile revolution the cloud computing revolution and you have a recipe for progress or disaster. What makes cloud computing an ideal candidate for using emerging technologies, encouraging employee productivity, and improving communications is the technology behind it. Cloud computing can make use of virtually any type of application or software. When mobility is combined with cloud computing, productivity gains as well as the security risks abound. Harnessing the power of these technologies while securing corporate assets will challenge IT departments for years to come.
Personal Devices Take Root in the Enterprise

BY FRED DONOVAN

Perhaps the best known impact of mobility on the enterprise is the bring-your-own-device (BYOD) trend, which is being spurred by the explosion in the number of smartphones and tablets being sold worldwide. According to a study by the research firm IDC, IT spending on smartphones surpassed spending on PCs in 2012 for the first time in history. People and companies are buying smartphones and tablets instead of PCs, which has resulted in a long-term decline in PC purchases.

Employees are bringing their smartphones and tablets to work in ever greater numbers. While companies first resisted, many are now embracing the move by employees to use their own mobile devices at work.

A full 85 percent of enterprises now allow their employees to bring personal mobile devices to work, and 70 percent of IT professionals surveyed believe that their company will be at a competitive disadvantage if they do not allow BYOD, according to a survey by IDC and smartphone maker Samsung.

Today, there are three mobile devices — whether corporate or employee owned — for every enterprise user, and this number is expected to climb to seven devices for every user by 2016, based on research by ZK Research.

These devices include smartphones and tablets running various operating systems, such as Windows, iOS, Android, and BlackBerry, and made by a range of manufacturers, including Apple, Samsung, Nokia, ZTE, LG, Huawei, Lenovo, Sony, Motorola, BlackBerry and more.

Despite the increasing acceptance of BYOD, IT decision makers, who are responsible for managing and securing all of these devices, have different views about BYOD priorities than employees, who want ease of use, according to the IDC-Samsung survey.

For example, half of IT decision makers believe that mobile access to enterprise applications and resources is an important consideration in a BYOD strategy, while only 28 percent of employees think access to those things are important.

At the same time, close to half of employees think the ability to share large files over mobile devices is important, while less than one-quarter of IT decision-makers think so. Many IT managers are worried that use of public file-sharing applications, such as Dropbox, could lead to loss of confidential data.

On security, a full 84 percent of IT decision makers think securing mobile devices using mobile device management solutions and encryption is critical, while only 74 percent of employee think security is a critical consideration.

Chenxi Wang, vice president and principal analyst for security and risk at Forrester Research, observes that enterprise challenges from BYOD are “multifold.”

One set of challenges is operational in nature. “Once you give people email access, they want more. They start asking for back-end enterprise applications. This leads to a lot of operational changes to your infrastructure,” says Wang. There are four main operational challenges enterprises must face when it comes to BYOD: demand for additional network capacity to handle all of the mobile devices, help desk overload from employees calling for help with personal device problems, need to redesign enterprise applications for personal mobile devices, and the requirement to monitor and control personal mobile devices along with corporate-owned devices.

Joshua Wright, an independent information security analyst, says BYOD is an “upside down change” for many enterprises. “We are losing control with BYOD devices.

The introduction of smartphones are driving more complex demand for data, not just email, calendar and contacts – users are looking to do whatever they could do on a PC on these mobile devices.

Some organizations see this...as an easy financial decision of allowing employees to bring their own devices, that way they don’t have to pay for the devices or the services. What a lot of organizations quickly discover is that BYOD can actually cost more.”

According to a survey of 250 IT professionals conducted in 2012 by security vendor Lieberman Software, two-thirds of respondents believe that BYOD increases costs, due to the added security measures required to lessen those risks.

Phillip Redman, research vice president at Gartner, notes that personal mobile devices were not designed to support enterprise needs. “The introduction of smartphones are driving more complex demand for data, not just email, calendar and contacts – users are looking to do whatever they could do on a PC on these mobile devices,” he says.

Data loss is a big risk for enterprises, Wang notes. Employees use their mobile devices to process corporate data, and this could lead to data loss if the right security precautions are not taken.

In the case of the loss or theft of a personal mobile device, enterprises should have the technical capability to remotely wipe the device. Unfortunately, for only 10 percent of smartphones, an enterprise can be sure the data has been successfully wiped, says Wang.

Data-stealing malware also poses a threat to corporate data and could result in the compromise of privileged accounts.

The risk of malware is greatest on Google’s Android, according to the study conducted in March 2013 by security firm Trend Micro. The research found that 15 percent of Android apps were infected with malware, and 22 percent of the Android apps leak user data.

By contrast, BlackBerry has a reputation for strong security. The new BlackBerry 10 handsets integrate with the BlackBerry Enterprise Service 10, which provides mobile device management and security. The BlackBerry Balance feature enables separation of corporate and personal workspaces on the BlackBerry device, which prevents employees from transferring corporate data to their personal workspace.

Apple also has a solid security reputation for its handhelds, operating system and app marketplace. Unlike Google, Apple vets all applications before they are made available on its App Store. A full 60 percent of enterprises Gartner has talked to have plans to switch to Apple’s iOS as their primary platform in the next 12 months, says Redman.

“The BYOD train has left the station. We recommend that you embrace diversity and manage it. Just don’t stick you head in the sand,” Redman concludes.  

Once you give people email access, they want more. They start asking for back-end enterprise applications.
A More Collaborative Workforce
With Mobile

BY PAM BAKER

Not so long ago, mobile devices were used primarily as a means to check in at the office while workers were traveling. Today, mobile devices are the new work station. And that is seriously rocking IT’s world.

“Users will do whatever they have to do to get the job done with or without IT’s help or permission,” says Ira Weinstein, senior analyst and partner at Wainhouse Research. “The reality is that we gave information workers the burden of being constantly available and productive, indeed, to work all the time. It’s not fair to limit or dictate how they go about doing that.”

While it may come as a shock that these workers are so willing to casually wreak IT’s stringent security and compliance efforts, the truth is that there is nothing casual, nor malicious, about how workers choose collaborative tools for their mobile devices.

“Rogue users are actually the very people who push the envelope and drive the processes users are driving,” explains Weinstein.

Stay in communication with users and learn who they need to communicate and collaborate with and why they choose and like the tools they do. “Online third-party file-sharing services, like Dropbox, have become very popular and are often free, fast and easy to use,” explains Joe Moriarty, global vice president at Content Raven. “Employees can simply sign-up for the cloud-based service and begin sharing documents internally and externally with whomever they deem appropriate.”

Moriarty adds that “giving up control of proprietary corporate data to the cloud is troubling, especially a part of the cloud that the business itself doesn’t possess.”

And that’s exactly why IT must develop a partnership with users and work in tandem with their goals. continued on page 11

Equipping an Increasingly Mobile Workforce

RAPIDLY CHANGING MOBILE LANDSCAPE

The pace at which the mobile device market is growing is astonishing. IDC predicts the smartphone market will grow by nearly 50% this year, and the number of these phones in use will surpass 450 million. Meanwhile, the market continues to fragment as diverse manufacturers vie for market share. According to Gartner, the iPhone, Android, Blackberry dominated mobile market will see changes in the coming future, the most prominent of which will be Windows market share growth. In light of this fragmented mobile market, it is important that enterprises avoid tethering their strategies to a single mobile operating system. Additionally, the share of tablets in work environments is poised to grow dramatically and impact corporate environments. Gartner expects 80% of businesses to support a workforce using tablets by 2013.

FASTER SPEED, BETTER WEB

Other drivers that push mainstream adoption of mobile technologies will be advancement in connectivity speed and availability of a more powerful mobile web experience. Improved 4G connectivity means that most employees will gravitate to new mobile devices, as it will be much faster compared to their legacy phones.

The advancements in mobile web will make mobile the one-stop channel to obtain information and even make transactions. Mobile’s share of Internet traffic worldwide has been growing rapidly and in just 8 months it has bounced from 1.8% to 7.7% in 2011. This means each organization’s workforce will use their mobile devices for Internet browsing and transactions and will tend to limit the use of desktop machines to more complex tasks.

INCREASING BYOD ACCEPTANCE

As the trend toward BYOD in the workplace accelerates, the questions surrounding it have largely shifted from ‘whether’ to ‘how’ to support employees’ use of personal devices at work. BYOD is indeed becoming a mainstream practice, whether governed by IT or not. Many organizations are recognizing that they can use mobile applications to drive end user satisfaction and flexibility, simply by taking advantage of the constantly advancing capabilities of new smartphones. Mobile phones have also become powerful tools in enterprise systems environment. Employees are now able to carry a vast array of operations on a 4” inch screen “on-the-go” — from documenting and reporting an accident on the field to submitting an expense report, to capturing a new opportunity and updating a sales pipe-line — all without ever having to turn on their computers.

Gartner predicts that 90% of companies will support corporate applications on personal mobile devices by 2014. Not only will new apps be built and deployed for enterprises, but traditional web applications will also increasingly become available for mobile as well. According to MGI Research, by YE2014 over 40% of all enterprise applications will have a mobile app.

It is imperative that companies understand the opportunities BYOD create, craft the right strategies to deal with the challenges and capture those opportunities, and align the right resources to implement it in the most efficient way.
Teleconferencing on the Move

By Pam Baker

It is only logical that teleconferencing would come to mobility, but that’s not to say it has done so logically. “Many mobile apps for conferencing services have been web-based client portals that have been shoehorned into a mobile app,” explains Marc Beattie, managing partner at Wainhouse Research. “These legacy implementations still exist at some telcos, where product development lags behind independent specialists.” Nor have all new teleconferencing features been perfected for mobile use. “Mobile video is the big hype right now,” says Ira Weinstein, senior analyst and partner at Wainhouse Research. “It will fall back down and find new usage once its best use has been determined.” This means that companies need to be careful in selecting teleconferencing tools for their mobile workforce in order to avoid excessive spend on overhyped features and from getting locked into less than desirable tools and services. The good news is that there are plenty of options from which to choose. “Increasingly we are seeing mobile conferencing apps that are purpose built to the operating system, e.g., iOS, Android, and the experience is really superior,” says Beattie. “Nearly every major conferencing provider has a mobile app, including InterCall, PGi, BT Conferencing, and Arkadin. Additionally, there are some newcomers with original ideas that really ease the challenges of joining from a smartphone – these include MobileDay, UberConference, CrowdCall, and Call U Conferencing,” he adds.

But don’t forget to check with your existing teleconferencing provider for mobile options too. Often companies are unaware of the mobile features their current provider offers. However, if your conferencing provider’s mobile capabilities fall short of your needs, you do have other options. “If the app or capability is lacking with an existing provider, seek out a specialist who has an intuitive app that unifies mobile contacts and calendars for one-to-two click call setup for moderators and call entry for participants,” advises Beattie. “In any organization 20 percent of the power users typically use 70 percent of the volume, so if a user needs to add services for mobile, it may be smarter to have a dual provider strategy – one for heavy mobile users, and another for everyone else.” Also consider other collaborative alternatives, since mobile teleconferencing may not be ideal in all circumstances. “Mobile solves a problem, i.e., it makes you accessible when you otherwise wouldn’t be,” says Weinstein. “But videoconferencing on a mobile phone isn’t the best thing to use if you’re on a beach in swimwear or on a crowded subway with lots of noise and colorful characters.”

In other words, sometimes collaborating in text is better than full surround sound and unpredictable or unprofessional visuals. But there are other times when real-time voice communication supplemented by digital content and even video are the best means to communicate and collaborate. In such circumstances, nothing else will do in the user’s eyes. If your organization has not already established a mobile teleconferencing policy and tool set, users will make their own choices. “The advent of BYOD [bring your own device] has turned the tables on IT, and users have much more power in determining what they use,” says Beattie. “With that said, IT operates best when it pilots different services with small groups of users from the larger user groups, e.g., senior executives, sales, marketing, engineering. Gaining buy in and involving users in the decision will go a long way in keeping most users with the company ‘standard.’” Fortunately, there are a number of things happening in the mobile world that are likely to help corporations contain, control and also encourage collaboration efforts in their organizations, chief among them is unified communications.

“Collaboration services will likely move to mobile much more quickly with the advent of unified communications,” says Beattie. “Microsoft Lync 2013 and Windows 8 Mobile are slick implementations of real-time UC&C [unified communications and collaboration] in a mobile device – Lync and Windows 8 provide the same experience across desktop, tablet and mobile. Our hope is that Google and others follow with equally compelling implementations.” Once the static clears on all of these tools, businesses will benefit from incorporating them into their mobile strategies.

“Choosing a teleconferencing solution that merges human interaction with digital content is ideal,” says Kira Salem, director of marketing at Personify, an enterprise software company. “When these two components are married, audiences – which include current and potential clients – tend to stay more engaged than with content alone.”

Videoconferencing on a mobile phone isn’t the best thing to use if you’re on a beach in swimwear or on a crowded subway with lots of noise and colorful characters.
Cloud computing and mobility are natural partners given that both have such “be anywhere, do anything” natures. The particulars on that partnership are still being refined, though, before the marriage can be declared consummated. “Over time, things will consolidate into unified communications (UC),” says Ira Weinstein, senior analyst and partner at Wainhouse Research. “What’s coming is a centralized, coherent communications system, and then we’ll be off and running, but today we walk.”

So what will truly cloud-powered mobile look like eventually? For one thing, mobile user interfaces will become even more simplified, and, for another, content and conversations will roam freely between devices. “Mobile workers, for example, should be able to seamlessly transfer a videoconferencing session from an Android-based tablet to an iOS-based smartphone without missing a beat,” says Joe McGarvey, strategic marketing director at GENBAND, an IP multimedia application and infrastructure solutions provider.

But for now, enterprises are working with data and communications in the cloud on a more piece-meal basis. That’s as scary to IT as it is freeing to users. At the moment, users are tapping the cloud to find apps on their own that suit their individual workflows. And IT is busy trying to figure out how to secure company data, despite this onslaught against its carefully crafted security and compliance efforts.

“It’s nearly impossible to block ‘bad cloud’ apps versus ‘good cloud’ apps,” says Steve Barone, president and chief executive officer (CEO) of Creative Breakthroughs (CBI), an IT advisory services, risk management and network security company. So what can IT do to protect company data in the cloud and on mobile?

“If you can’t block, you have to build a model to secure,” explains Barone. “First, secure data where it’s stored. This includes databases, directories, file systems, and more. Secondly, secure it when it moves by encrypting those channels. Thirdly, secure it as it is being used. You can accomplish this by limiting users, data and applications.” Considering company data is fragmented and stored in silos in both the cloud and on-premise programs, companies are often

Employees need to be able to access and search all corporate sources of information, no matter their location or device or where the data is stored.
Your job is to now think less like an IT person and more like an end user.

"The problem with many social and collaborative offerings today is that they sit in a silo and as a result, business value or adoption is hard to measure or achieve," explains Sameer Patel, global vice president and general manager of enterprise and collaborative software at SAP. "Many are great at letting people connect, but they miss the important business context that sparks purpose-driven collaboration, and as a result, social applications suffer from limited adoption. A well-designed and purpose-driven collaboration strategy ensures a social foundation across all applications, people and data."

Most employees will accept a tool swap if the alternative is equally easy to use and useful for their purposes. But, to get them to swap to a more acceptable tool means it can no longer afford to commit to purchasing such technologies without user input and approval in advance. To do so will, without fail, lead to IT circonvention.

"This calls for a change in IT mindset. Remember end user experience and workflow is now a top priority," says Weinstein. "Your job is to now think less like an IT person and more like an end user."

That doesn’t mean IT has to, or should, relinquish all control. Indeed, that would be foolhardy. But it does mean collaborating with users on selecting tools and educating them on the why and how after a choice is made.

"Everyone has a favorite cloud storage provider or document-sharing site, but using 12 different tools can lead to major version control issues," says Dan Waldinger, director of marketing solutions and services for Brother, a hardware provider. "Companies with teleworkers should select one collaboration tool that all employees, whether in the office, at home or on a mobile device, can connect to. This way everyone has the most up-to-date version of important documents, and everyone is working with the same information."

Use training, awareness campaigns, and company policy to drive home the security message. "Keep policies as open as possible. Guidelines are good but actual policies are tougher," says Weinstein. "Look to instigating retroactive regulations, by which I mean let employees know that you will empower them to make choices, but you will be scrutinizing their decisions afterwards on their adherence to specific company requirements such as security and compliance, among other things."

And what of employees who still use collaborative tools willy-nilly, despite your efforts to be accommodating? "That means you have the wrong employee, not the wrong policy," says Weinstein.

Companies must determine where the sensitive data is, bring it together for centralized control and then make sure that continued work doesn’t create more segregated data locations.

"In a nutshell, companies must determine where the sensitive data is, bring it together for centralized control and then make sure that continued work doesn’t create more segregated data locations," says Barone. "It’s brutally tough and requires strong management."

A cloud provider with a strong commitment to security can help further protect data stored in the cloud. As to which solutions a company should use to support its mobile workforce and subsequent steps it should take to protect data, Barone offers these five tips:

1) First, get all key stakeholders in a room. A mobile security strategy that maximizes the benefits of bring-your-own-device (BYOD) requires input from everyone—not just IT. Human resources, legal, financial, operations, IT and executive management all need to be involved.

2) Second, before taking a reactive approach, companies need to assess their current security situation. Understanding where data is and how easy it is for employees to access it will lend major clarity.

3) Third, once issues have been identified through the assessment, the “fixable” problems should be addressed before proceeding further. Most data loss is the result of careless mobile use or an avoidable user error. This simple step can go a long way in repairing the situation.

4) Fourth, policies and procedures should be put in place to sustain security. Examples include mobile device “hygiene,” mobile ID access limits and responsible password practices. Employee training and ongoing management of mobile devices are critical to minimizing the security exposure through BYOD.

5) Finally, put a disaster recovery plan in place. Not all mobile security issues are related to data leaks. It could simply be employee misuse—like tweeting confidential information from a client site. A response plan that includes a communications strategy is required.

While securing data in the cloud and on mobile presents serious challenges, the potential benefits of combining the two is hard to overstate. "The real value of this hasn’t come to be yet," says Weinstein. "But, the more we regulate it, the more we strangle creativity and innovation."