dimension data

Five Major Trends
in Enterprise Mobility

Mobile technology has revolutionised the way we live, work and play. But for much of its history, mobility has been driven by consumer preferences, forcing enterprises to adapt.

As the cost of mobile voice service declined in the 1990s, cell phones went from being a luxury for the rich to an everyday device that people grew to depend on. The average monthly cellular bill dropped to $39.43 from $98.02 and the number of subscribers in the U.S. grew from 1.2 million to 69.2 million in the period between December 1988 and December 1998, according to CTIA – The Wireless Association. That's a more-than-50-fold increase.

The new century saw the widespread adoption of mobile text messaging: The number of text messages sent in the U.S. grew to 2 trillion in 2010 from 81 billion in 2005. That decade also saw the introduction of mobile email, first on the Palm Treo in 2002 and then on the BlackBerry. Not surprisingly, the average monthly bill grew from $39.43 to $50.07 between 1998 and 2008.

The market changed again in 2007 with the introduction of Apple's first iPhone, which fundamentally changed people's expectations of what they could do while mobile. Almost 220 million iPhones have been sold worldwide since then.

While the focus of the wireless industry has been on the consumer market primarily, mobility has had a major impact on the enterprise as well. Enterprise users were the first to adopt mobile voice and mobile email, though those services eventually expanded to consumers and features were calibrated for their use. Since the iPhone revolution, the industry focus has been decidedly consumer.

For the past five years, enterprise IT departments have been under increasing pressure from users to expand the range of mobile devices they allow to access enterprise email and other applications. Given the lack of security capabilities companies had come to expect with the enterprise-grade BlackBerry devices they had been supporting, IT departments were reluctant to ease restrictions. However, with pressure coming from C-level executives and business unit managers, most organisations have now expanded the supported range of devices – both company-supplied and user-owned – to include Apple and in some cases Android as well.

We have a few stellar examples of companies that integrate mobility well: Federal Express transformed not only its own company, but its entire industry with the revolutionary adoption of mobile terminals. Companies like PACCAR, manufacturer of Peterbilt and Kenworth diesel trucks, has integrated mobile technology into their products in enormously creative ways. But enterprises have only begun to scratch the surface when it comes to capitalising on what mobility can do to transform business processes.

This white paper examines the key trends in enterprise mobility over the next 12-18 months, the drivers of those developments and what enterprise IT departments should anticipate.

Contents

BYOD Hype Takes Center Stage

Probably the single most discussed issue in enterprise mobility of the past five years has been the push from users to bring their own devices (BYOD) to work and access corporate email and other applications.

A recent CCMI survey on BYOD found that 60% of respondents follow a corporate liable policy and that despite all the noise, only 10% of respondents have a pure BYOD policy in place.

The survey also found that the primary drivers behind a pure BYOD policy are employee satisfaction, improved productivity and lastly cost reduction. And while the first two are hard to measure, the key finding of the survey was that- so far – BYOD policies have not resulted in any cost savings among the survey respondents.

A recent InformationWeek Survey on Mobile Security also provided some unsettling insights into how IT departments are preparing – or not preparing – for the challenges posed by BYOD policies.

Many IT groups have swung the pendulum too far in favor of accommodating user requests. Regardless of who owns the device, securing corporate data, systems and assets are still core IT responsibilities. The same can be said for managing and supporting information technologies that can make employees more efficient, productive and accessible. It does not appear that all organisations making the move to BYOD are investing sufficiently in the tools or procedures they will need to ensure a positive outcome.

While the threat of lost or stolen devices was recognised as a top mobile security concern by 84% of respondents to the Information Week survey, 43% reported that the requirement for on-device data encryption "varies by device type, ownership, and approved use." This flexibility is too lenient. On-device encryption should be a hard and fast requirement if there is any corporate data or emails residing on the device.

On-device encryption **should be a hard and fast requirement** if there is any corporate data or emails residing on the device.

Some 26% required hardware encryption (the preferred approach), "if it was supported by the device." Again, while acquiescing to users' requests can be a morale booster, encryption is one of the issues that should not be open to negotiation. The top reasons cited for not requiring on-device encryption were "lack of management sponsorship" and a lack of staff "skills to manage encryption on mobile devices." This is not all that surprising given that mobile management is still a relatively new field and up to a few years ago it was more a purchasing than an IT function.

In terms of tools to manage mobile devices effectively, only 25% of organisations have invested in mobile device management systems, though another 31% plan to implement them in the next 24 months. So it seems clear that before a BYOD policy is adopted – or even a BYOD hybrid policy – an effective mobile device management system along with lock down security measures is a must.

Some 40% of enterprises are counting on users following mobility policies with no means of monitoring or enforcing compliance. Only 20% check for mobile malware on all platforms. It is only a matter of time before a mobile catastrophe strikes and an enterprise security breach is splashed across the news. Whether through malware sneaking onto the phone or a user simply leaving a device without a password in the back of a cab, sensitive corporate data can fall into the wrong hands and possibly expose the company to regulatory fines or worse.

While some enterprises are embracing the BYOD trend, many have not taken the steps security professionals would consider prudent to secure and manage the data and devices.

The Mobile UC&C Non-Event

IP PBX and unified communications and collaboration (UC&C) vendors continue to tout the importance of mobility, yet almost nobody is buying their mobile UC capabilities. That would include the cellular-based solutions (i.e., Cisco Jabber, Avaya oneX, Siemens OpenScape Mobile, NEC MC550, Mitel UCA, etc.) or the dual-mode Wi-Fi/cellular variety (i.e., ShoreTel Mobility, NEC uMobility). While mobile is a big focus in UC, UC doesn't even register as a topic of discussion in mobility!

At face value it appears that a mobility component for UC would be a sure win. Most users divide their time between their desks and the mobile environment, and the type of flexible connectedness offered by UC&C with presence, directory access, IM and conferencing should have value for mobile users.

The problem: IP PBX and UC&C vendors are limited by the APIs the different mobile operating systems make available, so it is virtually impossible to deliver the type of tightly integrated user experience people have come to expect from consumer apps.

Those who try to pitch the cost savings of shifting mobile calls to Wi-Fi face a second problem in that many enterprise IT managers – rightly or wrongly – assume their Wi-Fi networks cannot support voice adequately. They fear that pushing a solution on the user that works worse than cellular voice service only exposes them to more criticism.

The widespread availability of wireline and wireless IP-based broadband networks also **can further enhance an organisation's productivity**.

But enterprise reluctance to adopt mobile UC&C solutions might be for the best, because mobility in conjunction with consumer-oriented social networks could offer an appealing alternative to enterprise UC. One of the biggest reasons we find users ignoring the mobile UC&C offerings is that the same capabilities exist natively in their smartphones. That would include things like clicking a number in a document to dial a call, integration with the directory, click to join a conference and so on. Frankly, those native capabilities in the phone work much more smoothly than the mobile UC&C kludges.

Market research firm eMarketer reports that roughly a third of mobile users access social sites today and that percentage will reach 42% by 2014. In a similar vein, iPass in its Rise of the Social Enterprise 1Q 2012 reports that 85% of LinkedIn users and roughly 28% of Facebook users use the services for business purposes. That's a lot more than are using enterprise social networks like IBM's Connections or Cisco's Quickr. While concerns about security and the appropriateness of those public services remain, we are already doing BYOD, why not "Bring Your Own Social"?

The Role of Tablets – End of the Desk Phone?

The other mobile device that is roaring into the enterprise is the tablet, led by Apple's iPad. Tablet sales increased 150% last year, and likely will top that figure this year with options like the $199 Kindle Fire.

For the moment, tablets are being used in the enterprise for basically for the same things as in the consumer environment: reading emails, texting, web access, playing games and watching videos (if the boss isn't around). According to Google, most tablet use occurs at home, but the appeal of the tablet's user interface leads people to look for things they can do with them. Unfortunately for business users, creating content is not easy to do on a tablet.

Hoping to capitalise on the trend, IP PBX and UC&C vendors are rushing to figure out how to better integrate tablets. Some decided to build their own, like Cisco with the Cius and Avaya with their Desktop Video Device.

Cisco added its own security software (a good move as the Cius ran the Android 2.2 operating system, one not favored by enterprise security managers) and sold the tablet with a stand that allowed it to work like a desk set for voice or video calls with a built-in speakerphone. The user could pull the tablet element out of the stand and an in-progress voice or video call would automatically transition to the Wi-Fi network. Cisco announced in May that there would be no further enhancements to the product, moving instead toward the idea of developing software to integrate other tablets into its UC&C solution.

Avaya is still hanging on to the Desktop Video Device and marketing it as a high-end desk set with mobility capabilities and running its innovative Flare interface. In the meantime, Avaya has developed a voice-only version of the Flare interface for iPad and plans to do the same for Android tablets.

Lots of other vendors are developing video clients for tablets including Polycom, Vidyo, Damaka and RADVision (recently acquired by Avaya). All of this assumes that video will be a breakout application for tablets, a premise that has yet to be proved.

Besides Cisco and Avaya, most of the other UC&C vendors are developing software clients and, in some cases, hardware cradles to accommodate tablets. ShoreTel and NEC have shown prototypes of tablet cradles, though they demonstrate the hazards of jumping on someone else's bandwagon.

The problem is that if there is a case on the tablet (i.e., the first investment every tablet buyer makes), the tablet no longer fits snugly in the stand. If you've ever tried to remove one of those cases you'll know that people are not going to rip them off every time they get back to the desk. And that's with the tablets we already have. What happens if the next version is a little bigger or a little smaller and the connector is in a different place?

The big question remains: What are enterprise users going to do with their tablets and will they have any meaningful integration with the IP PBX/UC&C solution?

It is unlikely that tablets will be adopted as telephones unless walking around the office with a Bluetooth headset on suddenly becomes en vogue. If tablets do have a role in UC&C voice, there would need to be a UC&C client on the tablet, but when the user went to place a call it would be transferred to either a desk set or smartphone.

There is a better chance tablets could work for web conferences, in conjunction with either an audio or videoconference. Unlike a smartphone, the tablet has a screen large enough to display the entire image clearly, and to even allow the user to take control of a shared screen.

Machine-to-Machine: The Internet of Things

The other question raised by the tablet phenomenon is what is next on the horizon.

We have seen marvelous innovation in the mobile space over the past two decades. First there was the PDA, and then Handspring built a phone into its Treo and launched the smartphone revolution. Of course, they soon lost the lead to BlackBerry and its secure, enterprise-grade email. Apple shocked the industry with the introduction of the iPhone in 2007 and iPad in 2010, delivering a mobile experience that only a genius like Steve Jobs could conceive.

In the transition from the Handspring Treo to the iPad, the mobile market has shifted from being an enterprise-dominated to a consumer-dominated game. The most exciting mobile innovations are coming from the consumer space. Consider technologies that allow users to remotely monitor home security systems and the recharging of their electric vehicles.

These integrations are just the beginning of connecting machines to each other in the emerging Internet of Things. Enterprises already have explored this potential with wireless patient monitoring systems and infusion pumps, or in the automotive field with services like OnStar or Hughes Telematics, recently acquired by Verizon Wireless. This is just the tip of the iceberg, though.

The declining cost of power-efficient, chip-level radios and expanding range of high-speed wireless networks will provide capabilities that were simply unimaginable a few years ago. LTE already delivers downstream data rates in the order of 20 Mbps – faster than many home DSL connections.

In Wi-Fi, the next wave will be 802.11ac, which uses wider channels and more efficient coding systems to push the data rate over 1 Gbps. The first 802.11ac chipsets already are hitting the market.

There are also developments in shorter-range technologies like Bluetooth and its cousin Zigbee. The first applications for many of these will be in gaming and home

We have seen marvelous innovation in the mobile space over the past two decades. First there was the PDA, and then Handspring built a phone into its Treo and launched the smartphone revolution.

entertainment, but with the blurring of consumer and enterprise technologies, their appearance in the enterprise is inevitable.

More than new devices, we will see wireless technology embedded in more existing devices, and those devices will communicate with one another in new and interesting ways. One key is the ability for Bluetooth devices to automatically associate with like devices in close proximity, giving us the ability to intuit relationships between data, devices and individuals.

Take the implications for UC presence information, for example:

- If a smartphone is associated with a desk set, the network knows the user is within 10 meters of his or her desk.

- If the phone is associated with the office Wi-Fi network but not with the desk set, the user is in the office but not at my desk.

- If the phone is on the office Wi-Fi network and associated with a bunch of other Bluetooth devices, the user might be in a meeting or in the cafeteria; identifying the closest Wi-Fi access point could clarify that.

- If a user is associated with the Bluetooth interface in his or her car, the user is not available for texting.

All of that information could be published with our presence status (if we choose to do so), to schedule calls or callbacks when status changes.

There is a threat of Big Brother in all of this, but with intelligent design and flexible user controls, we can be far more productive and effective. If you couple that intelligent mobility with the ideas emerging in the social networking space, we could be defining a new level of connectedness where everyone in organisations works together more effectively.

Getting Our Arms Around Android

Probably the most unpredictable element in the mobile marketplace is Android. Over the past three years the operating system has come from nowhere to surpass Nokia's Symbian, BlackBerry and even Apple's iOS to become the market leader in both the U.S. and around the world. Many think Apple is the world leader, but Android has more than double Apple's market share worldwide (50.9% versus 23.8%) when all manufacturers are considered, according to Gartner.

Despite its success, the strategy for Android remains murky. There are currently 10 different Android releases in circulation. The most prevalent is Android 2.3, which represents 64.6% of devices in use as of June 1, 2012.

The problem is that 2.3 does not feature native on-device encryption (though you can add it with products from companies like Good Technology, or 3LM). It also lacks a number of important MDM capabilities, leaving it significantly less secure than the BlackBerry or Apple platforms. The first Android smartphone release that supports native encryption is 4.0, but that represents only 6.7% of the installed base. Further, there is no assurance that existing phones will be able to install future operating systems.

The multiplicity of releases is generally referred to as Android fragmentation, but that's just one manifestation of the problem. Each device manufacturer puts its own wrapper around Android, changing the user interface and making each implementation slightly different – Amazon removes elements like Google Maps, for example. Think of what that does to training and support costs!

On top of that, Android has become the poster child for mobile malware. Juniper Networks estimates that there was a 472% increase in Android malware in the second half of 2011.

Contrast that to the approach taken by Apple. Where Android phones are sold primarily through mobile operators, Apple uses that channel as well as its own retail stores. Even if you do buy the iPhone through the operator, all of the software and updates come from iTunes (unless you jailbreak the phone), and you can stop in at the Genius Bar in the Apple Store to resolve any problems. So while the operator may distribute the iPhone, Apple is responsible for support. Apple also vets all of the applications distributed through the iTunes store, and while a few bad apples (no pun intended) have slipped through, its track record on squelching malware has been stellar.

RIM has largely done the same thing for its platform, and Microsoft took the same route with Windows Phone. While the earlier Windows Mobile operating system had a mess of incompatible versions (to the point that each application had to publish a list of the devices it would work on), with Windows Phone, Microsoft adopted the controlled distribution approach. The devices are distributed by the operators, but the software and ongoing "touch" is from Microsoft.

It will be interesting to see if the Android community can deliver that same type of consistency and security protection in the open environment. If not, one of the manufacturers may have to step up and deliver an enterprise-grade Android implementation that provides those assurances that are so important to enterprise buyers.

Will the Mobile Industry "Discover" the Enterprise Wireless Customer?

Enterprise users still play second fiddle in the mobile operators' and mobile device manufacturers' plans. But there are a couple developments that might finally get enterprise customers back into the mobile industry's field of vision.

First, the mobile industry is running out of options to pump more ARPU (Average Revenue Per User) out of consumers. The mobile operators' plan had been to get users on voice plans to get them hooked on mobility. From there, thanks in part to low-cost slide-out phones with QWERTY keyboards, texting at per-message or even flat rates delivers solid revenues. Data plans – automatically applied to most smartphone bills – are the real cash cows.

But mobile operators are running out of cattle to drive down that trail. More than half of the cell phones sold in the U.S. are now smartphones, and there is some percentage of the population who will never upgrade to smartphones. So with the ARPU accelerator essentially becoming tapped out, the mobile operators are going to have to find a new source for growth. And in the short term, that translates to getting growth from the base of smartphones already in place through packaging – and repackaging – data plans, some shared, to boost revenue.

As we noted above, machine-to-machine (M2M) applications are one source, but a lot of those applications are very low volume and minimal revenue per line. The operators had been hoping to tap into the tablet boom, however, industry estimates are that 75% to 80% of tablets sold are Wi-Fi only. Consumers have made it clear that they do not see the value in shelling out another $20 to $30 per month for a tablet data plan. Many have been predicting that the operators will start to offer multi-device or even family data plans, and Verizon jumped into that in June. That may boost revenues, though not at a rate on par with moving customers from feature phones to smartphones.

One serious move on the pricing front is to eliminate flat-rate data plans for the new higher-speed 4G services. Even Sprint, the last national provider to offer unlimited data recently announced it too is capping its data plans for mobile hotspots at 5 Gbytes.

The going rate for 4G is currently $10 per gigabyte. Casual users can get by with 1 GB, heavier users (lots of web surfing and streaming audio) might burn 2 GB, and mobile video freaks (one hour of video a day) can probably get by with 3 GB.

The hope is that out of desperation, mobile operators and device manufacturers will finally start offering services that are meaningful to enterprise users. Options include dual-number handsets, wireless Centrex, better integration with wired telephone and UC&C solutions, cost-effective FMC solutions (like Sprint's Mobile Integration) or per-use remote wipe and lock services. The operators have been offering mobile device management (MDM) services, but it is a low-key effort that appears to be having little success.

On the device side, RIM had always been seen as the premier enterprise mobility supplier (despite the fact that during its heyday 70% of its sales were to consumers), but RIM's demise has opened an opportunity for other handset makers.

Apple has done a very good job adding enterprise capabilities to its iOS operating system including Microsoft Exchange access, on-device encryption and important MDM APIs, but it is highly unlikely that company will alter its core consumer focus. Many still recall Steve Jobs referring to CIOs as "Chief Information Orifices" at a conference in 2005.

Motorola is now under Google's ownership, though Google has said repeatedly that it will not give the company any special advantage over other Android platforms. New CEO Dennis Woodside is a former mergers and acquisition lawyer who oversaw multibillion-dollar revenue growth in Google's advertising businesses. So the focus there seems to be on Google's figuring out how to make money on mobile advertising and not on better enterprise integration.

Probably the best prospect is Samsung, which has put together an enterprise sales group that works in conjunction with the mobile operators much in the same way RIM does. It's also headed up by a former RIM executive. Android, Samsung's operating system of choice, has been fairly weak with regard to mobile management and security features, but that's starting to change with Android 4.0 (code named "Ice Cream Sandwich"), so they could have a pretty good story to tell.

First, **the mobile industry is running out of options** to pump more ARPU (Average Revenue Per User) out of consumers.

Conclusion

The enterprise mobility market continues to grow and evolve, driven primarily by the requirements of consumers rather than enterprise buyers. But with the threat of BYOD initiatives, those two worlds are coming together. For enterprise mobility managers, this presents some daunting challenges. BYOD may lead to a wider range of devices, and a multiplicity of implementations – some of which are far more enterprise-ready than others; but lenient device acceptance without strong security policies is a recipe for disaster. Regardless of who owns the device, IT is still responsible for managing and securing corporate systems and data.

More enterprises are moving mobility initiatives to the front burner and developing systems and policies to ensure users get the productivity benefits of mobility while not exposing the organisation to undue risk. And the job is not going to get any easier.

Legal liability has yet to be explored, for the most part. Is the company opening itself to a lawsuit if it wipes out someone's baby pictures? If there is an e-discovery requirement, can the company take possession of a user's $600 smartphone for months as needed?

Enterprises are just embarking on this brave new world in mobility, and there are still plenty of issues that will need to be resolved. But the message is clear: The time to get started is right now!

About CCMI

CCMI provides specialised telecom data services and content-rich events to the communications service provider and enterprise markets. CCMI's enterprise information service delivers independent market research and analysis, tightly focused educational webinars, a thought-provoking podcast, and industry-leading conferences. Learn more at http://www.ccmi.com.

About Dimension Data

Founded in 1983, Dimension Data plc is an ICT services and solutions provider that uses its technology expertise, global service delivery capability, and entrepreneurial spirit to accelerate the business ambitions of its clients. Dimension Data is a member of the NTT Group. Our global footprint means that we have feet on the ground in 51 countries and can supply multi-vendor services across 140 countries. You get local business support wherever you are.

Dimension Data's proactive approach to Communication Lifecycle Management and our NexTEM application enables clients to save on communications costs today and optimise communications spend into the future. NexTEM captures your billing, inventory and usage data in a single platform, allowing you to see easily how you can optimise by managing all your fixed and mobile network services. This on demand self-service solution uploads wireless bills and automatically generates immediate cost and timesaving results – in minutes, not months. The single, cloud-based platform accommodates company growth without adding complexity and satisfies the full range of enterprise communications expense management requirements.

www.dimensiondata.com

About Communications Lifecycle Management

Communications Lifecycle Management is a range of services that optimize the full spectrum of your communications spend – from one end of your enterprise to the other, anywhere in the world allowing you to make timely, evidence-based decisions about the cost and utilisation of your entire communications network, not just bits and pieces of it.

The communications lifecycle is managed through NexTEM, a cloud-based application allowing you to take control of your voice, data, fixed, mobile, local and global communications costs across your entire organization.

www.dimensiondata.com/CLM

dimension
data