Mobility Temperature Check: Just How Hot Is BYOD?

Enterprises retain foothold in corporate-liable mobile environments but are also easing in support for employee-owned devices

July 2012

Commissioned by:

dimension data | xigo

Conducted by:

CCMI

Mobility Temperature Check: Just How Hot Is BYOD?

Enterprises retain foothold in corporate-liable mobile environments but are also easing in support for employee-owned devices.

Executive Summary

Powerful smart phones and tablet computers with fast wireless connections have made it possible for workers to be productive from nearly anywhere. However, the balance of power over device selection and procurement has begun to shift as employees clamor to connect their personal mobile devices to the corporate network.

IT and telecom groups accustomed to procuring, configuring and managing enterprise-class devices such as laptop computers and BlackBerry smart phones, as well as the applications that run on them, are now confronted with droves of small, untethered non-corporate devices. These devices might be running any of a half dozen or more mobile operating systems (OSs). Enterprises are trying to determine if and how to connect them to data resources securely and how to manage wireless expenses effectively in an environment that no longer contains network borders.

Mobility Lexicon

• **Corporate-Liable (CL).** The enterprise procures, manages and secures all end-user devices, paying all monthly network service plan fees.

• **Employee-Liable (EL), a.k.a. Bring Your Own Device (BYOD).** Employees purchase personal devices, use them at work and are responsible for paying the monthly network service plan fees. The enterprises might reimburse users for business-related network service costs via a flat monthly stipend in the user's paycheck or via expense report.

• **Hybrid.** A mix of CL and BYOD devices, which is likely to be the most common model in all but the utmost security-conscious organizations going forward. Enterprises are looking to new tools for provisioning, mobile security and expense management to implement top-down control regardless of who buys the device.

In short, corporate mobility – and, in particular, the "bring your own device" (BYOD) approach to device procurement – is turning the traditional approach to device provisioning, management and security upside down. The current climate could take much of the decision-making and control away from IT and telecom professionals. This could be a positive development for organizations obsessed with cost cutting, which is easily today's largest stated enterprise business goal. For example, the entrance of BYODs into the organization could offer economic relief to employers in terms of capital expenses (capex). On the other hand, the added security risks and administrative costs of network service plan reimbursements could offset those benefits, so enterprises have to evaluate all angles carefully.

To get a clearer picture of the corporate mobility situation and to determine enterprise goals, approaches and challenges surrounding these trends, CCMI surveyed 116 IT and telecom professionals nationwide in May 2012. The terms used in the survey were defined as shown in the box above ("Mobility Lexicon"). The key findings and analyses of those findings are below.

Key Survey Findings

» ***BYOD is in the ramping-up stage.*** The majority of enterprises, for now, still control device purchases, management and usage in a corporate-liable (CL) model. However, many have embraced BYOD in part, and, going forward, most anticipate running a hybrid CL/BYOD model to accommodate user populations with different requirements.

» ***The top three goals of BYOD programs are 1) to keep employees happy; 2) to improve productivity; and 3) to reduce mobile capex.*** The first two objectives are difficult to measure in hard terms. With regard to the third goal – the desire to reduce costs – nearly all respondents that already allow BYOD in their organizations said their mobile capex hasn't changed or has actually increased. In other words, ***BYOD has not reduced enterprise mobile capex costs.***

» ***Tablet computers are just registering on enterprise radars.*** Mobile phones still get the majority of enterprise attention, though a fair number of respondents envision tablets eventually replacing laptops and smart phones in the future.

» ***Organizations have made significant progress with mobile policy and control.*** Nearly all have written policies requiring user agreement about behavior that affects expense management, security and compliance, and two thirds have implemented special mobility software to assist in these tasks.

» ***Most respondents were confident that they understood and could control their mobility costs.*** This is surprising, given that the current, widening mix of devices, service plans and ownership models can create a mobility free-for-all that is challenging to track. This begs the question: ***are respondents' confidence levels accurate?***

Let's look a bit more closely at each of these findings.

Latest Liability Models

The traditional approach of corporate ownership and liability still reigns among respondents: the majority (60%) said that their organizations remain fully corporate liable at this time (see Figure 1). Still, a strong showing of respondents (22%) said they run a hybrid of corporate-liable and BYOD models to accommodate different populations of users. And 10% said they were fully BYOD shops that not only allowed users to use their own devices at work, but expected employees to pay all their monthly network service charges in full themselves.

Of those who allow some BYOD in their organizations – which constituted 40% of all respondents – more than half of those BYOD programs (54%) have been in place for two years or longer.

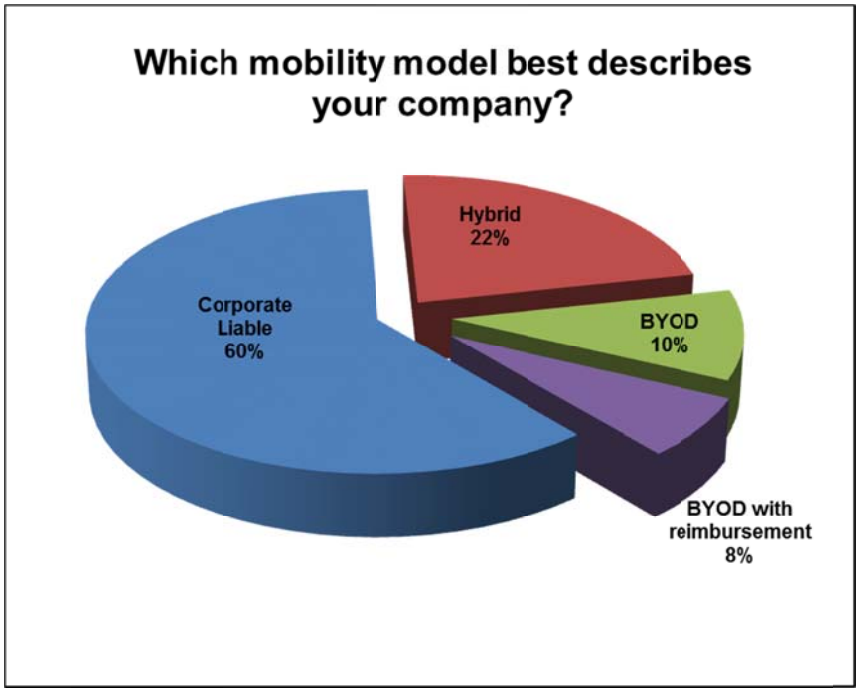

Figure 1: While the majority of companies remain fully corporate liable, a strong showing (40%) employ some form of BYOD.

Traditional Research In Motion (RIM) BlackBerry devices garnered the greatest amount of formal corporate support (27%), due largely to RIM's long-standing enterprise-class policies and security features and the industry's widespread IT expertise with the RIM ecosystem.

However, the emerging availability of enterprise-class solutions that manage and secure multiple mobile OSs from a single system has spurred a more than respectable ramp-up of IT support for non-RIM devices, too: 20% said they formally support Google Android devices; 18% said they support Apple iOS devices; and 13% said they support Microsoft Phone 7.

There are several reasons that these devices, initially built as consumer-class devices, are becoming blessed by corporate IT and liability models are changing:

- Mobile OSs are gaining enterprise-class security feature interfaces, which device-makers are opening up to developers. As a result, a number of security companies are building support into their multi-OS platforms that enterprises can use to provision, secure and control a variety of devices from a single system.

- Enterprises, understandably worried first and foremost about security issues pertaining to BYOD, are starting to feel these mobile management and security products have matured enough that they can do a good job controlling their mobile environments, according to 14% of those surveyed.

- Pressure is at hand from incoming new hires accustomed to living with their mobile phone or tablet of choice at their sides 24/7. They can't conceive of having to juggle separate devices for work and personal use. This has employers scampering to create a friendly and flexible corporate culture while finding ways to ensure compliance with internal and industry-specific compliance policies and to protect the security and integrity of corporate assets. The industry is stepping up to the plate to provide solutions.

How is all this activity affecting corporate spend? According to survey respondents, little has changed in their mobility spending – at least for now – although some incidents of increased expenditures were revealed by the study.

Spend Trends

Survey respondents indicated that the desire to create a friendly corporate culture topped their motives in allowing BYOD in their organizations (see Figure 2).

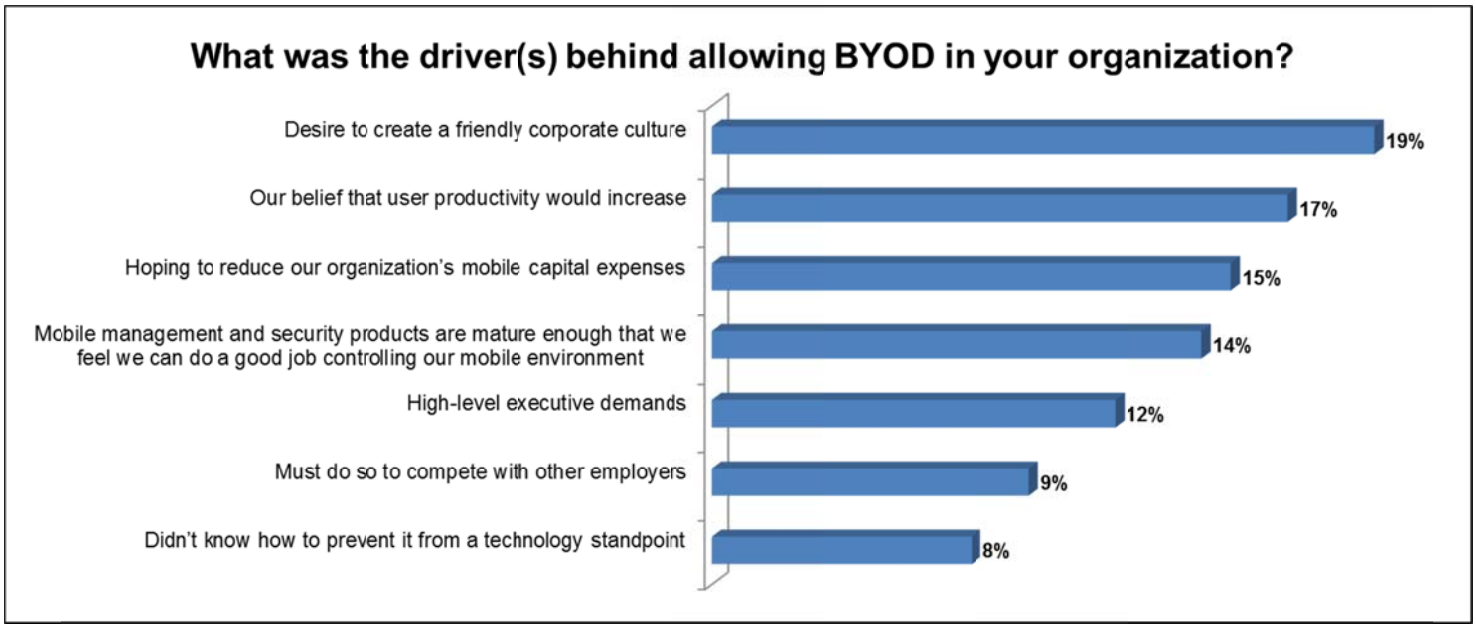

Figure 2: Reducing mobile capex came in third, after creating a friendly corporate culture and increased user productivity, on the list of reasons for allowing BYOD.

With corporate culture, productivity and capex reduction goals as the primary drivers behind BYOD programs, early reports don't have a definitive answer for whether these objectives are being met yet. As noted in the **Key Findings** section, reducing mobile capex ranked high on priority lists. However, two-thirds of respondents who allow BYOD in their organizations said that their mobile capex hasn't changed – and nearly a quarter (24%) said mobile capex had actually ***increased*** by more than 20% (see Figure 3).

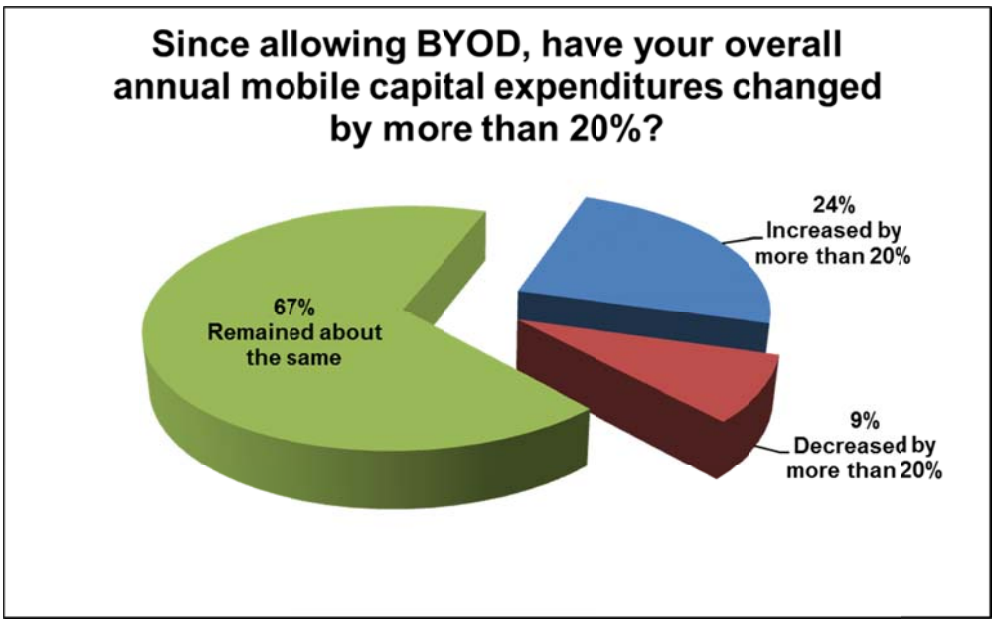

Figure 3: Though reduced capex was a top BYOD priority, the majority of respondents indicated no significant change in expenditures and nearly a fourth actually reported increases.

• ***Capex.*** With employees bringing their own devices to work, why would mobile capex increase? One reason is likely that there are so many mobile device types available – feature phones, smart phones, tablets, netbooks, laptops – that users are simply using more of them and creating more potential for employers to pick up the tab. A recent Cisco report estimated that the average number of devices carried today by employees is 2.8, a figure the company anticipates to jump to 3.3 by 2014.[1] Another potential reason is that most companies surveyed reported a mix of CL and BYOD devices. In some cases, it's likely that the volume purchasing discount with a given carrier has dropped so that the per-device cost of the remaining CL equipment has gone up.

• ***Voice/data service plan costs.*** A similar explanation could be applied to the cost of mobile voice and data network plan charges: Most say their network service plan spend has stayed the same (61%), while just shy of a third (30%) say it has increased by more than 20%. Again, the loss of volume discounts and opportunities for cost-effective pooling plans are likely to be affecting the network service charges. In addition, most U.S. carriers have dropped their "unlimited" data plans. The rescinding of the unlimited option means that cost-conscious companies still supplying CL devices for executives and others need tools for monitoring usage so that wireless bill shock doesn't occur at the end of the month.

• ***Help desk/support costs:*** Most respondents (70%) say their support costs haven't changed, while between a fourth and a third (28%) say those costs have increased by more than 20%. By rights, users who bring their own devices to work shouldn't automatically expect technical support from their IT staffs. On the other hand, what is the support staff supposed to say when users experiencing connectivity problems or performance degradation come calling? Respondents imply that they are doing their best to support a multi-OS mobile environment, particularly since it's not necessarily evident to the end-user whether the cause of problems lies in the device itself, the public cellular network or in the corporate network. With the user owning the device, the mobile network operator running the cellular network, and corporate IT running the internal enterprise network, the potential for finger-pointing and wasted troubleshooting efforts runs high.

• ***Employee subsidies.*** Most respondents say they reimburse their employees for business-related mobile phone calls and data access. The method used by employers to reimburse employees for mobility costs is

[1] Cisco IBSG Horizons Study, May 2012

fairly evenly split between a flat monthly stipend (47%) and reimbursement via expense report (41%). Both approaches have their pros and cons: the flat stipend represents a fixed and budgetable cost and, once a system is set up and in place for it, requires little in the way of ongoing administration. The opposite is the case with monthly expense report reimbursements. On the other hand, the monthly expense report approach reimburses what is actually spent, rather than an estimate. And it can be difficult for enterprises to determine how much of a fixed stipend to provide: too little, and it doesn't satisfy users; too much, and the savings potential of BYOD drops.

How much respondent companies subsidize varies widely, but most fall between $26 and $75 per user per month. Slightly more subsidize in the $51 to $75 range (26%) than in the $26 to $50 range (22%). For context, at one extreme, 16% percent spend more than $1 million on mobile subsidies (including related administrative costs) and 9% aren't sure just how much they spend in subsidizing BYOD users (see Figure 4).

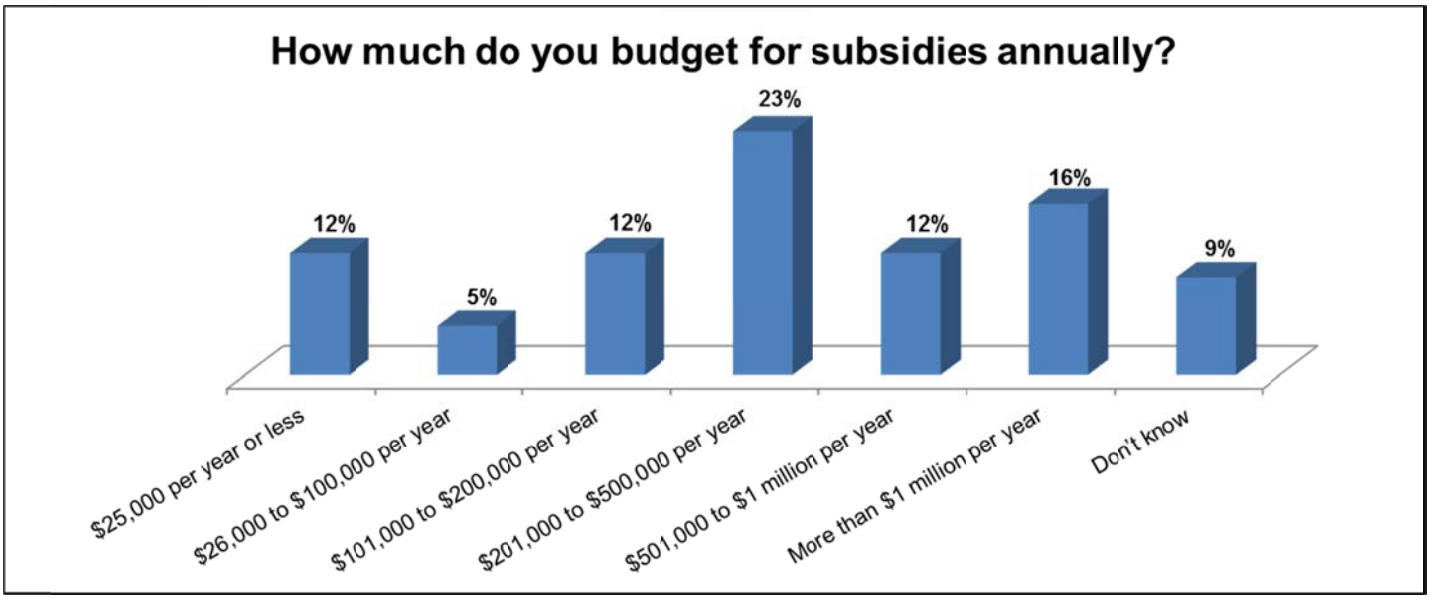

Figure 4: The amount enterprises subsidize users for their voice and data plans varies widely among respondent companies. Most subsidize users between $26 and $75 per month, spending between $201K and $500K per year, including related administrative costs.

• ***Mobile phones vs. tablets.*** In terms of which devices enterprises will purchase or subsidize, mobile phones are front and center at this juncture. More than half (59%) of respondents said their companies have different procurement and reimbursement policies for tablets and mobile phones.

More respondents are likely to purchase a mobile phone (15%) for employees than a tablet (5%) and are also more apt to subsidize more for mobile phones (50%) than they do tablets (30%). In terms of monthly service plans, they're also more likely to pay all business-related charges for mobile phones (65%) compared with tablets (55%).

The reasons for this can be chalked up, in part, to the relative newness of tablet devices; smart phones have a good two-year jump on them. In addition, enterprises have long been reliant on – and comfortable with – the use of basic or feature-phone handsets for voice, and the jump to a smart phone doesn't seem as drastic. In addition, tablets tend to be known for their powerful capabilities in conferencing and video streaming. These are beneficial to many enterprise communications applications but also carry the risk of severe overages should users download movies and other high-bandwidth applications, often without realizing the economic consequences, now that unlimited data plans are rare.

Still, when asked how they viewed tablets, well over a third (36%) said they saw tablet computers as a possible replacement for laptops in some or all of their organizations (see Figure 5).

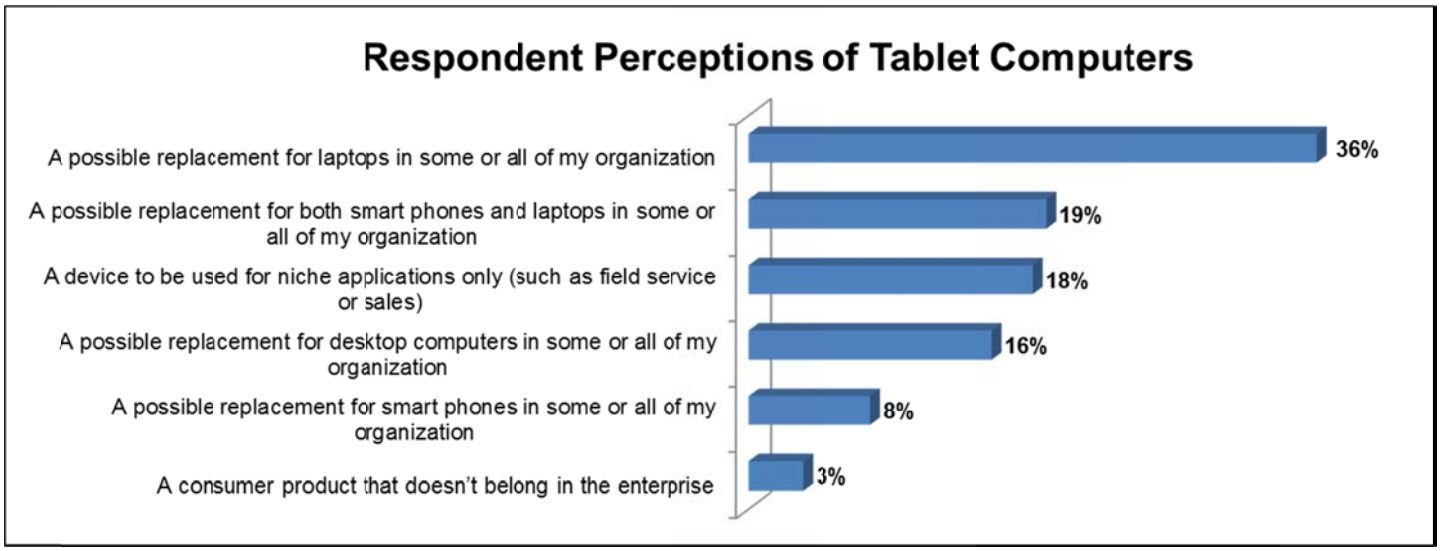

Figure 5: Well over a third (36%) of survey respondents said they saw tablet computers as a possible replacement for laptops in some or all of their organizations.

• ***Spending confidence levels.*** Respondents expressed reasonably high confidence levels about their understanding of how much their companies were spending on wireless products, services, operations and administration. Between 82% and 85% said they were "very confident" or "moderately confident" about what they were spending. These highly positive results could be related to one or both of the following:

» As noted in the **Key Findings** section, many enterprises have at least started down the path with policy-setting and enforcement using automated third-party mobility management tools, which helps them keep track of – and potentially curb – usage-related spending.

» As is notoriously the case when companies have external security audits conducted, organizations might firmly believe that they have a strong handle on their aggregate spend, but are surprised – and thus have not accounted for – any number of hidden costs that a third party (or third-party tool) might uncover.

Policy and Control

Survey takers reported significant strides with policy-setting and enforcement. More than half (52%) said they have a written mobile usage policy in place that mobile users must agree to and sign as part of their mobility management process. Two thirds indicated they are using automated tools from one or more mobile device and expense management suppliers to help enforce the policies and handle other functions.

Those who have not deployed such tools cited expense (34%) as the top reason. In addition, security will likely always reside near the top of the list of reasons for enterprise BYOD hesitation. BYOD has headed into the mobility spotlight during a time when financially motivated organized cyber break-ins are coming into their own, and regulatory compliance issues, if anything, have grown more stringent. Enterprises fret about opening up their networks more during a time when risks and potential fines are greatest, but also recognize that they have little choice if they want to satisfy higher-level executive demands (cited by 12% of respondents as a driver), compete with other employers (9%) and aren't sure how to prevent BYOD (7%).

Conclusion and Recommendations

Amid wide reports of a BYOD “explosion,” the enterprises surveyed indicated that they are still easing into their support for employee-owned devices. Many have done a good job laying the groundwork, with policies in place that cover security, compliance and expense issues, and two thirds are using tools from one or more suppliers to help enforce those policies and automate other capabilities.

Most enterprises have little choice but to open up their network environments to additional devices as employees themselves grow more savvy about how to use their personal devices for corporate access; it’s IT’s job to make sure that this access is clean and secure. Fortunately, alongside the many mobile device types and form factors has emerged a new genre of automated tools to help enterprise IT identify device types, enforce policies and track and control usage. The tools can be implemented in a variety of ways – on-premise hardware appliances, virtual services or, perhaps most conveniently, in the form of software as a service (SaaS), also known as a cloud service.

Before evaluating and selecting tools, enterprises should identify user groups and classify them into corporate- and/or BYOD (employee-liable) policy groups. Highly mobile international travelers, for example, might be one group with quite detailed usage policies associated with it, given that the potential for going over budget intensifies considerably as users cross country borders. Have employees sign off on the policies to ensure that they understand the security and usage issues at stake and have given permission for the organization to install security software on the employee’s device. It is important to make sure the employee is on the same page as the company on this, as IT control over a personal device can have security and liability ramifications in both directions, whether the employee leaks corporate data from a personal device or the enterprise wipes personal data from an employee’s device to protect its own assets.

About Xigo
Xigo, a Dimension Data company, instantly reduces and controls mobile, fixed and global telecommunications costs for organizations of all sizes. The company provides the first solution that uploads wireless bills and automatically generates immediate cost and time-saving results – in minutes, not months. Xigo's single, cloud-based platform accommodates company growth without adding complexity and satisfies the full range of enterprise communications expense management requirements. Xigo's success is attributed to customer-centric innovations and industry firsts with more than a decade of expertise spanning wireless and wire line communications. For more information visit www.xigo.com, email info@xigo.com or follow us on twitter @XigoNow.

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. www.dimensiondata.com.

About CCMI
CCMI is the industry's leading provider of telecom rate and data solutions and information. We are dedicated to delivering relevant, highly specialized and strategically focused content. Find a complete product listing at http://www.ccmi.com/Products. CCMI publishes *Voice Report*, the leading independent source of telecom news, analysis and award-winning guidance on communications technology services and equipment for the enterprise. For analysis and guidance on the latest telecom happenings, visit http://www.TheVoiceReport.com, and sign up to receive email updates.

About Joanie Wexler, Contributing Editor
Joanie Wexler is an independent editor and analyst in Silicon Valley, Calif., who has spent more than 20 years analyzing trends and news in the computer networking industry. She covers the gamut of IT hot topics, including data and voice network services and equipment, convergence, wireless communications and data center trends. Contact Joanie at joanie@jwexler.com