HDI®
The IT Service & Technical
Support Community

The Mobility Revolution and Its Consequences for Support

by

Roy Atkinson
Senior Writer/Analyst, HDI

UBM
TechWeb

Contents

Executive Summary

Based partially on data collected for the HDI Research Corner report "Supporting Mobile Devices," released in December 2010, and on other cited research, this white paper seeks to understand the shift to mobility and its consequences for the support center, as well as point out some best practices currently in use and some trends in the development of support mechanisms.

This mobility revolution has far-reaching consequences for the workforce of the future, but it is also a part of global mobility and virtualization trends in the larger sense.[1] The demand is high, the change is rapid, and the future is largely unpredictable. Tomorrow's devices may change today's IT thinking. High-level executives may make decisions based on the "cool factor," resulting in security and support questions that IT must answer, and answer quickly. Changes in work rules, such as work-from-home and the emergence of virtual workers and teams, are part of the revolution. Mobile devices are an integral part of the distributed workforce.

The current trends in mobility indicate that this "revolution" is far more than the collective voices of insistent IT customers saying, "We want our iPhones/Droids/BlackBerrys/Windows Phones/iPads, and we want them *now*!"

The mobility revolution discussed in this white paper is only one part of a much larger sea change taking place in the business world, most of which will have an impact on IT in one way or another. This sea change involves remote and virtual workers, travel, collaboration, security, budgeting, HR considerations, availability and capacity planning, staffing, and more. In short, the support center needs to be a part of a larger rethinking of how, when, and where IT provides support, what is supported, and how access control and security can be provided in an environment that, in many respects, is not of IT's making.

The white paper is divided into the following sections:

- An introduction, offering information about the scope of the mobility revolution;
- A look at the current state of the technology in flux;
- Guidance on specific ways organizations can think about managing their own mobility revolutions; and
- Conclusions.

[1] Union Network International, "The Global Mobility Revolution" (2004), http://www.andrew-bibby.com/pdf/Global%20Mobility.pdf.

Introduction

> We have to accept that workers are no longer chained to their desks and not always using company issued computers. Regardless of operating system, hour-of-day or location, employees will be sweating to meet deadlines and help desks will need to support them.[2]

It's the day after the New Year's break at work, and calls are streaming into the service desk:

- "How do I connect my iPad to the department's shared drive?"
- "How do I view a presentation on my new BlackBerry?"
- "What's the best app for editing Word documents on my iPhone?"
- "How does this Droid app connect to our central database?"

And what's worse is that *only one* of these hypothetical callers has a mobile device that was purchased by the company and is listed as "supported" by IT.

If you were to state many companies' policy about supporting personal devices in a slightly different way, what you'd be telling your end-users is, "We're sorry, but our policies do not allow for you to be more productive. You'll have to choose between the following alternatives: Sit at your desk to wait for the quarterly sales report, or go to your daughter's soccer game. You cannot do both." Of course, both the employee and the company know quite well that yes, you *can* do both. That smartphone is perfectly capable of connecting to the company's e-mail servers, but the company doesn't own the tools to properly manage it as a network client, or to ensure the destruction of important data should the device be lost or stolen. The employee *could* go to the soccer game and get that sales report on her phone, "if the IT department would only let her." Likewise, you might gladly work at home for an hour or two in the evening if only you could use your iPad to read and reply to all the work e-mails that seem to pile up, while simultaneously updating your Facebook page with news about the kids. But your company does not support your device or allow it to connect to any company resources.

Later in the day, you happen to walk past your friend Mark's cubicle. Mark is a fairly tech-savvy guy; you overhear him saying, "Sure…I just set up a rule in Outlook to send all my e-mail to my Google Mail account, and I get it on my BlackBerry from there. It's easy."

[2] Doug Mueller, "Supporting the Mobile Workforce," *SupportWorld* (Nov/Dec 2009), p. 35.

There appears to be a tug of war going on here, and it's growing more difficult by the day. On the one side is IT, trying to deliver on promises to the business that its data will be secure, that it will comply with regulatory obligations like HIPAA (the Health Insurance Portability and Accountability Act) and SOX (the Sarbanes-Oxley Act of 2002), that its hardware will be standard and inexpensive, and that its resources will be protected and available to those who are authorized to use them—and to no one else. On the other side are the employees whose workload has increased, who face the demands of parenting their children and caring for their parents, and who would like nothing better than to work both smarter *and* harder, given the tools to do so. They know that at home, technology is powerful and easy to use, while at work it's often slower and more difficult.

It is an undeniable fact that wireless mobile communication is the new standard. Forty years ago, when you said to someone "Call me," you meant, "Call my house" or "Call my office." You dialed up on a landline and called a location, not a person. Some years later, it became fashionable to be "in the car" when taking a call. The shift to mobility had begun. With the tremendous growth of the mobile phone market in recent years, you no longer call the home or the office or the car: You simply call the person. This has been a subtle but fairly rapid paradigm shift. The wires are disappearing just as that old bastion of communication, the phone booth, did. What's more, unified communications systems can make the boundaries between office, airport, hotel, and coffee shop simply disappear.

We are in the midst of another paradigm shift, and this one also has to do with mobile devices. Phones are no longer just used for talking and texting, but for browsing the web, taking pictures and video, staying on top of e-mail—both personal and business—getting directions, checking in with family and friends on Facebook, scanning barcodes, comparing prices, sharing thoughts and information on Twitter, checking stocks, and so on. Top companies have raced to produce productivity-increasing clients and apps for these "smartphones." One needs only to browse the iPhone App Store under the Business or Productivity category to see how many applications exist for that platform; likewise the Droid, the BlackBerry, the iPad, the new Windows Phone.

As organizations have become more focused on standardizing hardware and software in the interest of saving precious budget dollars, personal mobile technology has exploded. Hand-held, Internet-connected devices are omnipresent.

The impact of mobility cannot be overstated. In an August 2010 paper, Good Technology states:

> No longer bound by the walls of corporate headquarters, business professionals equipped with industry leading wireless hand-helds and software are increasingly able to do business anywhere, anytime—with instant mobile access to all corporate information and applications. Those enterprises that embrace and manage wireless convergence will realize improved productivity and increased competitive advantage.[3]

In every support environment, from higher education to health care to manufacturing, mobility can be a benefit to both productivity and profitability, but it can also be a treadmill of keeping up with rapidly changing platforms and applications.

To get a good picture of the rate of expansion of the mobile device market, one need only look at the sales of smartphones globally for 2009 and 2010. Citing a report by IDC, Computerworld reports that, "For the first three quarters, vendors shipped 200.6 million smartphones, an increase of 67% over the 119.6 million shipped for the first three quarters of 2009."[4]

There's also some rather daunting information available regarding the future growth of both the PC and the mobile device markets. "Shipments of smartphones, tablets, and other app-enabled devices will overtake PC shipments in the next 18 months, an event that may signify the end of the PC-centric era."[5] The article goes on to say that the PC market will continue to expand, but the mobile device market will overtake and surpass it. This means that the support center is likely to be involved in supporting multiple devices per person. For example, an executive may carry a company-issued laptop and BlackBerry, but may also wish to use an iPad for reading e-mail and news, and keeping up on social media while on aircraft or ground transportation.

In the HDI Research Corner report, "Supporting Mobile Devices," released in December 2010, almost half the respondents say they are struggling, and that

[3] Good Technology, "Managing the Mobile Enterprise" (August 2010), http://www.good.com/trygood/vzw/managing_the_mobile_enterprise_vzw.pdf.

[4] Matt Hamblen, "Smartphones grow by 90% in third quarter, IDC says," *Computerworld* (November 4, 2010), http://www.computerworld.com/s/article/9194963/Smartphones_grow_by_90_in_third_quarter_IDC_says.

[5] Patrick Thibodeau, "In historic shift, smartphones, tablets to overtake PCs," *Computerworld* (December 6, 2010), http://www.computerworld.com/s/article/9199918/In_historic_shift_smartphones_tablets_to_overtake_PCs.

is where the most attention should be paid. For the purposes of this paper, we are defining "mobile devices" as *smartphones and tablet devices available to the consumer as well as the business*. We are not discussing hand-held devices like the "guns" used to scan barcodes in stores, warehouses, and factories, or tablets that are basically modified laptops; none of these were included in the HDI survey.

The Current State of Technology: Rapidly Accelerating Change

IT departments, though accustomed to rapid changes in technology, are struggling to keep up with the pace of mobile device adoption. Frequent mobile operating system updates change the capabilities of these devices, adding encryption where there was none, facilitating connections to Exchange and other broadly-used e-mail systems, installing VPN (virtual private network) technology, and so on. A good-faith IT policy, which may once have disallowed connection because of some technical shortcoming, is out of date today because that shortcoming no longer exists. What's more*, enterprise leaders believe that they will not be using the same mobile technologies in two years*. According to an MIT Technology Review Business Impact Report, more than half of the enterprise IT decision makers surveyed are using BlackBerry, but expect a shift to the iPhone (34%) and the Droid (28%), and a drop in BlackBerry's share to 25 percent.[6]

Historically, the IT department would find a new technology that might, in its view, benefit the organization, and it would plan to implement that technology, driving change from IT outward. Now, both line employees and leaders within the business are driving the changes. A new technology arrives on the market; people buy that device and begin using it at home or on the road, where they discover that it is easy to use and has benefits beyond the technologies offered at the workplace.

Employees *at all levels* want to use mobile technologies, and want to use them *now*. In a Cisco survey in the UK, fully two-thirds of employees feel that they and their employers could significantly benefit from technologies that allowed them to work remotely, and that they would put in extra work time—*up to four hours a day*—if they had the capability. The employees said that they *expect* access to "networks, applications, and information anywhere at any time."[7] Of course,

[6] Mark Lowenstein, "The 'Bring Your Own Device' Policy," *Technology Review Business Impact: The Mobile Enterprise* 1.2 (November 3, 2010), http://www.technologyreview.com/business/26634/.

[7] Ashdown Group, "Employees 'want to tap into mobile technology benefits'" (October 22, 2010), http://www.ashdowngroup.com/news/employees-want-to-tap-into-mobile-technology-benefits--news-800136491.

this raises questions far beyond the scope of the technology itself. There are HR considerations, such as overtime, differentials, work-at-home policies, and so on. But essentially, *employees want to be more productive*, and they have the means to do it, literally in the palms of their hands.

"Why is technology so easy at home and so hard at work?"

Those of us in the IT world know that not all wishes can be granted, at least not easily. Decisions must be made about how to set firewall policies, which VPN technologies will be used, which applications should be accessible from the Internet, and so on. Employee policies take time to write, modify, and approve. On the other hand, for technical management of mobile devices, new applications must be acquired or built to manage these connections. Audits may be required to ensure compliance with HIPAA, SOX, PCI DSS (the Payment Card Industry Data Security Standard), and other regulatory systems. Corporate security must be considered carefully, to prevent rogue access to employees' personal and corporate financial information. As we also know, most people do not care *how* a computer works, only *that* it works. Likewise, employees do not care to know what goes into making either IT policies or support happen; they just want it to happen. Moreover, they want the thrust of those policies and technologies to be *enabling rather than inhibiting*.

In light of the change mechanisms required, even the 45 percent of respondents to the HDI survey who have policies in place and the additional 44 percent who are developing them are almost certainly aiming at a moving target.

- More devices are coming to market. (Example: The Windows Phone recently released by Microsoft was not on the market when the HDI survey was active in early November 2010, and so could not be included.)
- Product updates and enhancements are occurring on shorter timelines.
- Many players are entering the mobile device management field.[8]
- Well-known providers are releasing products aimed squarely at the mobile security and data protection market.[9]

The situation is further complicated by the ease with which employees can bypass corporate systems and find ways around existing policies and pro

[8] "Mobile device management," Wikipedia, http://en.wikipedia.org/wiki/Mobile_device_management. *Note:* The list is not exhaustive.

[9] John Girard and Eric Ouellet, "Magic Quadrant for Mobile Data Protection," Gartner (September 2010), http://www.mcafee.com/us/resources/reports/rp-gartner-mcafee-mobile-data-protection-2010.pdf.

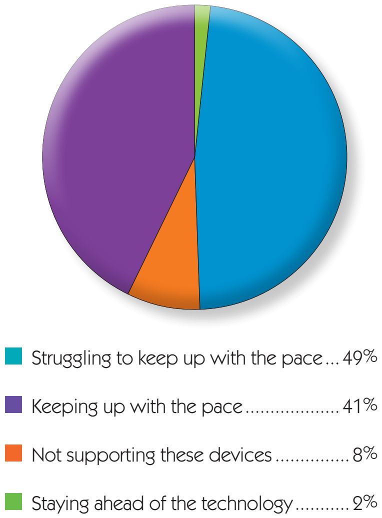
cedures. As noted in the reference to "Mark," tech-savvy employees will find a way, whether it is forwarding e-mail and calendar information to an online provider, or moving important documents into online storage they can access from their devices. And tech-savvy employees who are also laboring under increased workloads, as a result of hiring freezes, downsizing, or job aggregation, will be that much more motivated to find creative ways to work from home, the airport, hotels, on lunch breaks, and so on.

Regarding the technical aspects of mobile technology, what is true today will almost certainly not be true tomorrow. As we learn from Ray Kurzweil, "The paradigm shift rate…is currently doubling (approximately) every decade."[10] And this paradigm shift, as we shall see, may be profound.

The Current State of Support: Developing

According to the HDI Research Corner report "Supporting Mobile Devices," only 2 percent of respondents reported that they are "staying ahead of the technology," while 49 percent are struggling to keep pace, and another 8 percent have opted out of mobile device support. As mentioned earlier, 44 percent of respondents say their policies regarding mobile support are in development, while 45 percent say they have policies that are well defined.

How support organizations are handling the pace of emerging technologies:



Since 89 percent of respondents have policies in place or under development, while 57 percent are either struggling with the technology or have opted out, it seems fair to say that, by and large, the respondent organizations have chosen a policy-driven rather than a technology-driven approach. This appears to have some advantages. Policies are far less expensive to revise than infrastructure, and can be far more rapidly revised. The policies can be written to reflect the current infrastructure, and then revised as the infrastructure is replaced or upgraded, or as new technologies come into play. Of course, no policies are effective unless they can be enforced.

The key components of policies directed toward the use of mobile devices include:

- Having clearly stated security goals, communicated in a way that employees can understand;

[10] Ray Kurzweil, "The Law of Accelerating Returns" (March 7, 2001), http://www.kurzweilai.net/the-law-of-accelerating-returns.

- Providing for both company-owned and personal devices, though (perhaps) differentiating between the ways these devices are supported;
- Remaining general enough to provide for changes in mobile operating systems and capabilities; and
- Being specific enough to be effective and enforceable.

According to a Cisco report on the disconnect between IT professionals' perceptions of security policies and those of employees, "the methods used to communicate security policies to employees and the perceived fairness of the policies are critical to success."[11] Since one of the main considerations surrounding the support of mobile devices is security, the same statement could also be made about mobile device policies.

Companies also need to decide whether or not to support personal mobile devices, and, if so, which ones and to what extent. Some companies are extremely strict. At one well-known investment management firm, only company-issued BlackBerry devices are supported, while others have policies based more on the capabilities of the devices to encrypt data, connect securely to the company's e-mail servers, and be "wiped" remotely if lost or stolen.[12] Policies can be set using security criteria, and then decisions can be made as to which devices can or cannot connect based on those criteria, rather than by brand or operating system. Companies must communicate these policies clearly to their end users; likewise, they must be both willing and able to enforce those policies.

New mobile device management tools have entered (and are entering) the market in step with new mobile devices. Research in Motion (RIM) took an early lead in enterprise mobility, thanks, in part, to the BlackBerry Enterprise Server (BES), which allowed administrators to control the connections and capabilities of mobile users, and to secure organizational data. Because of the tremendous upsurge in demand for mobility, developers have been creating tools with similar capabilities for multiple platforms. These tools take away the "I'm sorry, but we can't do that" option for IT, but they also create increased budgetary and (possibly) staffing demands. If mobile device management was not included in budgets for 2011, companies will need to develop interim strategies for 2011, with an eye toward a complete mobility strategy in 2012.

[11] Cisco, "Data Leakage Worldwide: The Effectiveness of Security Policies" (October 2008), http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-503131.html.

[12] Lowenstein, "The 'Bring Your Own Device' Policy."

Guidance for the Support Center

Judging by the momentum and scope of the mobility revolution, rapid movement is not going to stop because IT support centers want it to, nor will it pause to allow support centers time to catch up. At current staff levels, will the support center be able to take on the additional work associated with the move to mobility? Before we can strike the proper balance between employee/executive demand and the support center's coping capability, we may need to ask a different question.

Sometimes changes come in unexpected ways. What if, tomorrow, your CEO decided to give iPads to every employee? This is not outside the realm of possibility. In fact, it has happened. Ashwin Ballal, the CIO at KLA-Tenecor, shared his story in a recent *Macworld* article:

> The happy CEO surprised the company's 5,400 employees by telling them that they would each be rewarded with a shiny, new iPad…While not officially supported as an enterprise device, the iPad would be allowed to tap into KLA-Tencor's network for e-mail, calendaring, contacts, web apps, and other purposes. Customer-facing sales and service technicians could use the iPad to access critical data over a virtual desktop… "That's a good 10,000 calls to the help desk," Ballal says. "We don't have the capacity to take that load."[13]

Ballal wound up seeking third-party tools to manage the tablets. His experience suggests that it is well worth becoming acquainted with the tools on the market and their capabilities *before* an executive decision changes the technology landscape.

In determining the type and extent of support your organization will provide for mobile devices, answer these general questions:

- Does the organization currently possess the mobility management and security tools necessary to provide the level of support to which the company has committed, through policies, procedures, compliance requirements, and service level agreements?
- Does the support center have the appropriate level of access to those tools, and/or a clear escalation path for resolving incidents and requests?
- Is information about mobile devices—at whichever levels of support are appropriate—included in the knowledge management system?

[13] Tom Kaneshige, "When the CEO gives iPads to all: One CIO's story," Macworld (January 27, 2011), http://www.macworld.com/article/157415/2011/01/companyipad.html.

- Are support analysts being appropriately trained to assist and to capture new knowledge?
- Are end users/customers aware of the support center's ability to assist them, the policies that exist, and their responsibilities to the organization?
- Are there consequences for violating organizational policies that clearly apply to personal mobile devices? (Does your acceptable use policy make it clear that personal devices connected to corporate network assets are subject to the same use policies as company-owned devices, or state what the differences are? Do end users/customers know the consequences of sending confidential data across insecure connections?)

Of course, once the strategic decisions have been made and the policies have been written, it's up to the support center to communicate those policies to the end users and to implement the organization's chosen type and level of support. These decisions can be broken down into three major implementation strategies: exclusion, limited support, and BYOD.

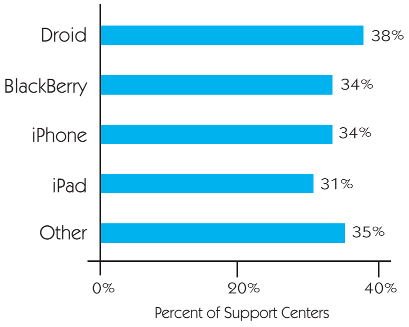
Strategy I: The Exclusion Approach

In this strategy, IT (in conjunction with the business) decides which devices it will support, which it will not support, and to what extent. This approach may work if:

- The organization issues a large number of mobile devices and fully supports them;
- End users are used to the necessary restrictions and disciplines involved in using their devices; and
- IT has rock-solid answers for everyone who asks for mobile support.

Roughly one-third of the respondents to the "Supporting Mobile Devices" survey said that they simply do not allow connections from personal devices.[14] Or, at least, according to their policies they don't. However, it is easy to circumvent even the most carefully considered policies if enforcing those policies depends solely on existing technology. For example, many—if not most—organizations provide a webmail solution. What is to prevent an employee, working through lunch at the local coffee shop, from connecting to webmail from a tablet or smartphone, and storing attachments either locally or in an online storage system?

Percent of companies that do not allow personal devices to connect to resources:



[14] Jenny Rains, "Supporting Mobile Devices," HDI Research Corner (December 2010), http://www.thinkhdi.com/bepartofthecorner.

For this type of strategy, robust firewall policies, network monitoring, and uniform policy enforcement are necessary prerequisites. If you want to protect your resources, you need to have ways to do it. In addition, the strictest policies may run the highest risk of employee noncompliance. Remember that people really want to be able to work remotely, and they may get pretty creative in the quest to do so.

Strategy II: The Limited Support Approach

In this strategy, IT clearly articulates the scope and limits of support for all devices. This approach can be effective if:

- The organization has a clear policy identifying the services that are supported for both company-issued and personal mobile devices;
- End users understand the consequences of bypassing the organization's security features; and
- Policies are universally enforced, in both the HR and technical senses.

Todd Wheeler, a global IT help desk manager, describes his organization's mobility policies this way:

> We issue BlackBerry as the standard corporate mobile device, but due to popularity and user requests, we've recently begun allowing iPhone 3GS, iPhone 4, and iPad users to connect to corporate e-mail. (Only these newer iPhone/iPad models are allowed due e-mail encryption capabilities. We do not support the Android platform.)
>
> Our users must purchase their own devices and service plans. iPhone users may return their corporate BlackBerrys and port their BB number over to their iPhone if they wish. Users who return their corporate BBs are eligible for reimbursement for their iPhone service (up to $100/month).
>
> As for support, our help desk analysts assist with e-mail configuration only. The users must maintain their own devices and service accounts with AT&T or their international carriers.
>
> We do have a "contract" or disclaimer presented to users that makes it clear that IT may send a wipe command to their personal device as we deem necessary (i.e., the device is lost, stolen, termination of employment, etc.). We do NOT allow iPhone and iPad users to connect to our network via VPN.[15]

[15] Posted by Todd Wheeler to the HDI Professional Association LinkedIn Group. Used by permission.

Todd's organization clearly states what the organization allows, what it does not allow, and what end users are responsible for. This approach to mobile device support is popular among organizations that do allow at least limited connections (e-mail only, for example) from personal devices.

Strategy III: BYOD (Bring Your Own Device)

There are some more radical thinkers who believe that it's time for a new understanding of support. In a recent interview with HDI, Scott Klososky, author of *The Velocity Manifesto*, said:

> It's very much time to quit setting standards and quit telling people what tools they are going to use. It's time to start asking them what they want, give them a budget, and let them go buy it. It's a simple concept. But not until you're ready to get enlightened, to realize that the most important thing isn't to set standards, to control devices, to control the software people use, it's will you be willing to let go and say, "Here's what you need to accomplish on your job. We don't care what tools you use—use what you need. If you love Mac, if you love the iPad, here's $2,000; spend it on whatever you want. Every year, we will give you another $500 to buy whatever new hardware or software you need."[16]

Can today's IT departments take this approach? Can we be what Mr. Klososky calls "enlightened"? What elements need to be in place for a BYOD strategy to work?

This approach can be put into place if:

- End users understand the implications of "nonstandard" device use;
- Support limits are negotiated and SLAs are drawn up or redrawn;
- Employees *at all levels* are held accountable for the security of organizational data and the confidentiality of communications;
- Communications about the security issues are open, clear, and direct;
- End users understand and agree to be "self-learners" of their chosen technology;
- The organization does not have any compliance requirements that preclude a BYOD approach; and
- The organization has the technology to ensure security and compatibility.

[16] "Social Ubiquity: What Are We Going to Do with It? An Interview with Scott Klososky," by Cinda Daly, January 2011, http://www.thinkhdi.com/files/dalyinterview/january_klososky.pdf.

Some very large companies are using this approach and proving it can work, given the right tools. They are leveraging new mobile device management (MDM) products to make this possible, which may not be practical for smaller organizations. One MDM company is producing a product that creates different spaces (a "virtual application environment"[17]) on the same device—one for business, one for personal use. This approach can offer the user lots of convenience and freedom, providing maximum access to internal systems and applications, while protecting the organization's security.

Another possibility is that the mobile devices will become part of a larger move to virtualization. In the "iPads to all" story referenced above, employees were able to take advantage of the virtual desktop. However, a rapid expansion in virtual desktop deployment would likely require the purchase of additional licenses, and the expansion of both virtual desktop capacity and storage.

Conclusions

The mobility revolution is not slowing down or going away. It is not merely a cry for cooler toys, it is a movement toward "work anywhere, anytime" capabilities across the organization. The proliferation of mobile devices will outstrip the demand for laptops (which themselves ushered in a new era for IT support), and will create many cases of multiple device ownership or possession. Medical records and charting software are now available for popular tablets. Some schools are requiring incoming students to have tablets for electronic textbook distribution and note-taking. Smartphones are getting easier to use, faster, and more powerful, and are putting unique capabilities in the hands of management, sales, and other personnel.

Support for the new, mobile world must begin with strategies that work, both from the employees' perspective (or they will just find a way around them) and from the IT perspective (or they will fail), especially regarding security and support. The support center is not in a position to create corporate strategies, but it should be fully engaged in discussions *regarding* the strategy. In ITIL parlance, there are broad implications across the spectrum of IT:

- Service strategy should take into account new ways of delivering IT services to the business and providing positive customer outcomes;

[17] Lowenstein, "The 'Bring Your Own Device' Policy."

- Service design should be aware of available tools, and groundbreaking ways to use them. Architectures and standards will likely require flexibility;
- Service transition may be fast-tracked to keep up with end user/customer demand and to provide the business with competitive capabilities; and
- Service operations should be prepared to handle new services or provide existing services over new channels.

Incidents involving mobile devices will affect the service desk, whether or not customers are using supported devices. (A customer may, after all, use an unsupported device to report an issue with a supported device from a remote location during nonstandard hours.) Problems involving mobile devices will likely require close relationships with wireless carriers and MDM vendors. Capacity planning should account for any expansion or acceleration of virtualization initiatives; financial planning should consider the MDM tools that best fit the organization's chosen strategy; and the project management office should plan future implementations accordingly. The need for clear, broad, and sustained communications from the support center will increase. Service level agreements (SLA), operational level agreements (OLA), and underpinning contracts (UC) must be updated, modified, or created to codify the appropriate levels of support that complement the organizational strategy. As the "face of IT" to the organization, the support center needs to gather, understand, and disseminate consistent information about policies and levels of support.

Mobile device support is, at its core, another service offered by IT to the organization; as such, it should be introduced using the same processes as any other new service. IT service management is broad enough to accommodate this new wave of technology. Just remember to focus on the *services*, not on the devices, because the devices will change rapidly.

Perhaps, someday soon, we will walk into the service desk and ask the same questions—"How do I connect my iPad to the department's shared drive?" "How do I view a presentation on my new BlackBerry?" "What's the best app for editing Word documents on my iPhone?" "How does this Droid app connect to our central database?"—but get clear responses.

About the Author

Roy Atkinson is HDI's senior writer/analyst. He is an HDI-certified Support Center Manager and a veteran of both small business and enterprise consulting, service, and support. In addition, he has both frontline and management experience. Roy is a member of the conference faculty for the 2011 HDI Annual Conference & Expo and is known for his social media presence, especially on the topic of customer service. He is also the outgoing president of the HDI Northern New England local chapter.

About HDI

HDI is the world's largest IT service and technical support membership association and the industry's premier certification and training body. Guided by an international panel of industry experts and practitioners, HDI is the leading resource for help desk/support center emerging trends and best practices. HDI provides members with a vast repository of resources, networking opportunities, and the largest industry event, the HDI Annual Conference & Expo. Headquartered in Colorado Springs, CO, HDI offers training in multiple languages and countries. For more information, call 800.248.5667 or visit **www.ThinkHDI.com**.