IT Managers Face Security, Management Challenges with Proliferating Mobile Devices

Since the emergence of the personal computer, IT managers have had to navigate through a computing and communications landscape where business and consumer technologies have intersected. Sometimes those intersections produce benefits for all involved; other times they result in destructive collisions.

For better or worse, consumer products and technologies today are exerting more influence than ever on the corporate IT environment. This "consumerization of IT" dynamic has become especially pronounced of late in the area of mobile devices and their burgeoning capabilities.

Laptop PCs have long been the dominant mobile devices spanning the business/consumer divide. In recent years, however, the proliferation of smartphones, tablet PCs and netbook PCs has increased the diversity and complexity of the mobility realm. Even IT managers who have successfully integrated laptops into their company's business processes and systems management regimes may now be struggling to accommodate — and leverage — this explosion of new mobile devices.

A recent survey of IT managers at mid-market companies (100-499 employees) conducted by IDG Research Services sheds light on the shifting mobile device landscape, and on the challenges they face. Those challenges spring from a number of sources, including the migration of "personal" device platforms into corporate settings, the popularity of multiple mobile operating systems, and the need to balance data and network access with data and network security. Not surprisingly, the security challenge ranks top of mind for most survey respondents.
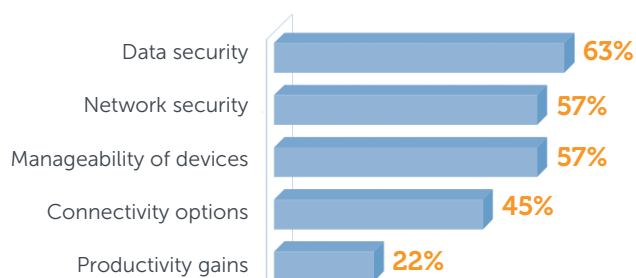
Top Mobility Challenges

Fully 63% of the IT managers surveyed selected data security as their top mobility challenge, while 57% said network security and device manageability were also top concerns. On the bright side, there are a number of technologies being built into mobile devices to address some of these security concerns. For example, Intel's Anti-Theft Technology, when incorporated into a laptop's design, can identify when a laptop has likely been lost or stolen (e.g., by excessive login attempts) and can automatically disable the laptop and prevent access to its data.
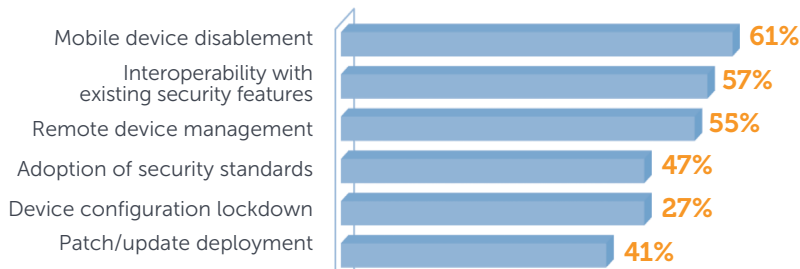
Advances in microprocessor technology are also aiding the mobile security cause. One of the most fundamental ways to secure mobile data is to encrypt it on the device, but such on-board encryption is very compute intensive, and can severely impact device performance. With multicore and multithreaded chips such as Intel's i3 and i7 Mobile Processors, however, mobile devices can perform other functions while encryption occurs simultaneously in the background, making this essential security measure much more practical than it has been in the past.

Beyond such on-board device technologies, the IT managers surveyed identified a number of security and management capabilities and features they deem critical. The single most-desired security feature is the ability to remotely disable mobile devices, a capability identified by 61% of the respondents. Other top management

FIGURE 1: What are the top challenges or barriers to supporting employees' personal mobile devices? Base: 51

Challenge	Percentage
Data security	63%
Network security	57%
Manageability of devices	57%
Connectivity options	45%
Productivity gains	22%

FIGURE 2: **What device management and security features do mobile technology vendors need to implement to become a trusted partner for your business?** Base: 51

Mobile device disablement	**61%**
Interoperability with existing security features	**57%**
Remote device management	**55%**
Adoption of security standards	**47%**
Device configuration lockdown	**27%**
Patch/update deployment	**41%**

and security features include interoperability with existing corporate security features (57% of respondents), remote device management (55%), adoption of security standards (47%), device configuration lock-down (47%) and patch/update deployment (41%).

Even the availability of desired security features won't be enough to convince some IT managers to let employees use their personal mobile devices for business tasks. "When dealing with corporate data, I want some control over that device," explains Doug Stoyko, director of information technology at the Winnipeg Airports Authority. The Airports Authority offers its employees a choice of either BlackBerry or iPhone smartphones, but doesn't allow its workers to use personal phones for their jobs. "What right do I have to kill your personal BlackBerry if I feel there's a threat for some reason?" Stoyko asks.

In related findings, the mobility survey revealed significant variability in how much employee input companies permit when it comes to selecting different categories of mobile devices. For example, when asked if their employees can select their preferred smartphone device, nearly one-third (31%) of the survey respondents indicated that choice is made solely by each user. Another 45% of respondents said that IT determines the mobile devices offered, but then gives employees the ability to select from approved device platforms or configuration options.

By contrast, in the case of laptop PCs, employee input is much more constrained. Only 6% of respondents say the decision of which laptop to use is made solely by the user, while another 37% say users can have input into the choice. Interestingly, the newer device categories of netbooks and tablet PCs fall somewhere in the middle when it comes to the level of user input allowed. But few respondents have yet to adopt either of these device form factors—35% of respondents say their organizations don't use

tablet PCs and 39% don't use netbooks.

That said, there are indications that the adoption of tablet PCs is likely to grow rapidly, driven both by the consumer success of Apple's iPad and the emergence of tablet competitors. Some new products, such as the Dell Latitude XT2 and the Dell Inspiron duo, are able to function both as tablet and laptop PCs, and are likely to prove popular in business uses that require the functionality of each form factor.

Durability, longevity key factor

Of course, IT managers must consider elements beyond a device's form factor and its on-board functionality when selecting an appropriate mobile product. For example, Vology Data Systems, a seller of new and pre-owned networking gear, is considering the adoption of tablet PCs that employees could use to interact with the company's CRM system. One of the candidate tablets is the iPad, according to Andy Swenson, vice president of information technology at Vology. Swenson likes and owns an iPad himself, but says he still needs to determine if the device is the best choice for Vology's corporate needs.

"Apple devices aren't as ruggedized as some laptops, so I have some concerns about the iPad's durability and longevity," Swenson says. He also says he must resolve whether Apple's "annoying" requirement for users to access applications via the Apple App Store could prove problematic. "If it's a closed platform and every time I need to do an update I need to work with the App Store, that won't work for me," he says.

Some of these same concerns affect the choice of Apple's iPhone as a corporate smartphone choice, but the IDG survey results indicate the iPhone is making business inroads. Research in Motion's (RIM's) BlackBerry device holds the top smartphone position, with 69% of the survey respondents indicating they support corporate-owned BlackBerry smartphones and 39% saying they support personal BlackBerry devices. Apple's smartphone comes in second, with 47% and 39% of respondents, respectively, indicating they support corporate-owned and personal iPhones.

Smartphones powered by Google's Android operating system ranked third in the survey (35% support corporate-owned Android phones), and Windows Phone 7-enabled devices ranked fourth (24% support corporate owned smartphones based on the Microsoft OS). That a quarter of respondents already support Windows Phone 7 is notable, given that the OS, and smartphones running it, first reached the market in October 2010. ∎