

How the iPad raises new concerns for mobile device security

Scott Lowe, Contributor

A decade ago, BlackBerry gave birth to a mobility movement. The fever grew as we relied more and more on laptops, but our addiction took new heights with the release of the iPhone and the iPad. Ten years ago, we would have never imagined that these devices would inspire such a thirst for mobility. Along with this great demand have come new opportunities and challenges in mobility management. In addition to Bring Your Own Device (BYOD) initiatives, organizations must now brainstorm new mobile workforce management strategies as well as consider new mobile device security threats and support models.

The mobile, always-connected tablet is here to stay -- if you doubt that, consider the sheer success of the iPad and the scrambling [competitors](#) are doing to get a leg up. Believe it or not, this can be a boon for businesses that are BYOD friendly. Although I doubt that many companies will simply stop issuing laptops anytime soon, the tablet is used as a complementary device in some circles. At Westminster College, our president has succumbed to iPad fever. He still has a laptop and totes it to some meetings but more often than not, he travels with just his iPad and is more productive than he was before. With proper iPad management, he's able to meet his "on the road" needs like keeping up with email, light document and presentation editing; watching the markets; and presenting information to potential donors.

However, his needs scratch only the surface of what's possible. Through vendor application stores, there are thousands upon thousands of [business apps](#) available. Further, with an appropriate infrastructure, applications can easily be decoupled from the desktop. Although decoupling has been possible with laptops for years, the new generation of mobile devices takes it to a whole new level, particularly when that mobile device has a continuous 3G network connection.

Let's talk about a few specifics:

- It's painful to watch a doctor lug around either a laptop or use a traditional convertible tablet PC to do his work. A more modern tablet with a streamlined health IT-specific user interface would be a major benefit to these organizations. A constantly connected machine means the doctor always has current information about my needs.
- Server and network administrators can carry a remote monitoring device to connect to the network so problems can be corrected. No laptop necessary.
- College students can now consume resources and access college-licensed applications as if they were in a traditional computer lab.

It would be impossible for me to list all of the possible benefits to the new mobility. Suffice it to say that "anytime, anywhere, any device" computing is here to stay and the sky is the limit. Dream big and then make it happen.

IPad, BlackBerry and iPhone device management

Although mobile devices can be used to leverage business opportunities in many ways, a strategy is needed to integrate BlackBerrys, iPads and iPhones into existing operations. Mobile devices are simply not going to replace thick laptops and desktops anytime soon. Further, the most popular devices, like iPads, BlackBerrys and iPhones, don't run key business applications. There needs to be a mobile device management process allowing organizations to make use of newer options while retaining critical legacy applications.

More mobile workforce management resources

[Mobile technology in health care now the answer instead of the problem](#)

[Ways to set the stage to encourage a strong mobile workforce](#)

Many mobile devices already connect to key business systems such as Microsoft Exchange and SharePoint, but unless vendors have taken steps to create "app versions" of their legacy applications, you're still going to face a hurdle. This is where another rising technology -- [virtual desktop infrastructure](#) (VDI) -- can fill the gap. Of course, other technologies such as Terminal Services can address this issue as well, but VDI brings other benefits to the table so it's the best fit for mobility use cases.

When coupled with the appropriate local app, VDI transforms a mobile device into a lean, mean business machine capable of connecting to any and all enterprise line-of-business applications. This provides the ultimate in flexibility. Users can leverage the benefit of mobility and not be left out of the office party. Even small-screen devices such as the iPhone can get into the game. VMware Inc., for example, creates an iPad version of its View app, and Wyse has a remote desktop protocol client that supports both the iPad and the iPhone.

Before you undertake a major mobile strategy, consider your whole spectrum of service offerings and determine which areas to modify that will best integrate your mobile efforts so they don't necessarily stand apart from everything else. Don't leave anything out.

The road to mobile device security

With your "new mobility" strategy in place, now comes the hard part: Oversight. Mobility adds new challenges and levels of complexity to existing processes and procedures. Suddenly, your network is being accessed by all kinds of devices that come at you from all over the place, around the clock. Mobile devices can also present unforeseen security and support challenges. Simply put, while the new mobility provides great opportunity, there are security challenges once applications leave the confines of the firewall. Among these challenges:

- **Prepare for lost and stolen devices:** Laptops were targets for theft, which is why we started using encryption and also why services such as LoJack were successful. A new mobile device should be treated just as seriously. A solid [mobile device security](#) policy will ensure that devices have lockout policies and can be wiped remotely in the event that

they're lost or stolen. More importantly, your mobility policies should include a provision that all devices -- including personal devices -- be wiped if necessary.

- **Keep devices current:** The primary challenge of new mobility is keeping up with current software releases -- a task challenged by the fact that the company may not even own the device. As a part of your BYOD policy, require that users adhere to software updates.
- **Modify support processes:** The help desk will at first resist supporting [employee-owned devices](#), so include it in the formation of your BYOD policy. Even if you don't allow BYOD, make sure your support processes lend themselves to supporting people on a variety of mobile devices that might reside on different carriers and run different operating systems.

It's safe to say that the new mobility is the way of the future. Organizations need to think big, execute well and provide oversight for this emerging space. With a little forethought, you can secure your space and embrace mobility management with open arms.

Scott Lowe is CIO of Westminster College in Fulton, Mo.