



J.Gold Associates LLC, 6 Valentine Road, Northborough, MA 01532, USA  
www.jgoldassociates.com +1-508-393-5294

## Mobile Security in Transition

***Mobile devices are clearly the darlings of business users who are acquiring them in droves, often despite corporate restrictions on doing so. The trend has so much steam behind it that about 25% of organizations (and the number is increasing) are now supporting user selected non-corporate provided devices. To be clear, not all devices are fully supported, nor have access to all of the back office apps available to users of corporate sanctioned devices. But it's only a matter of time until this capability expands. And there is no doubt business users' demands will increase.***

But there is a real threat looming on the horizon as organizations expand use of these partially or completely unsecured devices. And the threat expands dramatically when tablets are employed instead of less capable smart phones. Think of the amount of data a 64GB tablet can contain? Think about the amount of personal data (e.g., name, address, credit card, health records that can be compromised, or corporate secrets that can leak out (e.g., business plans, sales figures, product strategies)? Now look at the potential cost of such data loss. Aside from the potential for huge regulatory fines and customer defections, corporate competitive positions can be compromised. The Ponemon Institute estimates it costs a company \$258 to remediate each lost personally identifiable record. While some major and highly public data was lost in the past when laptops with 10s or 100s of thousands of exposed records vanished, is there any doubt that soon this amount of data will also be contained on corporate tablets making their way into the workforce with similar types of data?

So what needs to be done? Clearly data needs to be protected, but the best way to protect that data is transforming. In the past, data at rest on a device was encrypted to protect it from loss (Windows has this built-in and many third party products exist). Clearly this is an important and necessary security practice. But with a mingling of personal and corporate apps on the new smart devices, is this really the best way to protect data that could be exposed? No. Its too easy for me to copy the data from my corporate app which I just legally accessed over to my Gmail account and send it on to others. Or to copy it to an online app or cloud storage area once is decrypted and displayed. Encryption is not going away as it serves an important purpose (if the device is lost or stolen), but encryption alone is not sufficient. There needs to be a better way.

One way to do this is to not allow any data to be resident on the device. The device simply becomes a "Glass Window" to the data which resides in a protected space somewhere else. In fact, although not all users may like it, this is the approach that RIM is taking with the PlayBook,

where all data is resident on the BlackBerry device that is “Bridged” to it. But that doesn’t necessarily solve the issue of cutting and pasting data. For this we need another approach that controls what is done with the displayed data. New security measures will actually identify such cutting and pasting and/or forwarding to non-approved apps and prevent it from happening. The user can view and interact with the information locally, but not move the data without approval. While this seems burdensome to many, it is a good compromise if you are worried that data on the device may find its way to the personal side of the user’s apps and/or off the device and expose corporate assets. Of course this requires a level of control not currently implemented on most devices (like iPhone or Android) but it will make its way there before long in my opinion (and RIM is moving this way as well). I predict in the next 1-2 years, all corporate enhanced devices will have this feature.

Finally, one more level of security needs to be implemented, but will take a bit longer to get integrated. That is a virtualized platform approach whereby the business and personal sides of the device are kept separate in “walled gardens” and the transfer of data between the barriers is highly restricted. These virtualized stacks require a fundamental revamping of the OS (much as it has in the current PC and Server space) by adding hypervisors and specialized hooks into the processors (much easier to do now that we are moving into multi-core processors like those prevalent in tablets and higher end smart phones from NVIDIA, Qualcomm, TI, Intel, etc.). Virtualization is already being demonstrated by VMWare and OK Labs among others, and its popularity will grow quickly.

Security is one of those subjects about which people have many strong feelings and debates. Some want it to be relatively lax and primarily user controlled. Others want the extreme lock-down capability inherent in the most advanced and dedicated solutions used by the likes of President Obama. But what is clear is that organizations have a vested interest (and financial obligation) to protect corporate assets, and users have a vested interest in expanding the number and role of mobile devices they employ. It will be up to technology to find a balance, and corporations to decide what kinds of security to implement. What is sure is that this market is evolving rapidly driven by the myriad of devices being deployed, and companies will have to stay abreast of the changes for several years to come. And third party security providers will have lots of challenges ahead.

Jack Gold is the founder and principal analyst at J.Gold Associates, an information technology analyst firm based in Northborough, MA, covering the many aspects of business and consumer computing and emerging technologies.

***For more in-depth comments or analysis on this or other subjects, feel free to contact us.***

Jack E. Gold

[jack.gold@jgoldassociates.com](mailto:jack.gold@jgoldassociates.com)  
[www.jgoldassociates.com](http://www.jgoldassociates.com)  
508-393-5294

**Copyright 2011 J.Gold Associates, LLC. All right reserved.**