



Mobile Security: A Balancing Act

by Benjamin Wesson, Vice President of Product Management, Dexterra

Mobile computing has had an enormous positive effect on worker productivity worldwide. However, the flexibility, time savings and productivity gains that mobile computing affords must be balanced against inherent security risks. Some of these risks are obvious, such as the potential loss of company data from a stolen device or the possibility of data being intercepted in transit. Other risks from viruses/malware, over-privileged users and social engineering are often overlooked.

Yet despite the perceived importance of security, organizations are doing very little to secure mobile access—they're either waiting on the sidelines until viable security solutions present themselves or they're crossing their fingers and adopting a "hope for the best" approach. In fact, a recent survey of SearchMobileComputing.com members indicated that 31% of them have no mobile security policies in place at all. (See searchmobilecomputing.techtarget.com/news/article/0,289142,sid40_gci1277383,00.html for full survey results.)

Fortunately, enterprises can significantly improve their mobile security by utilizing a two-factor authentication scheme that verifies both the user's credentials along with the user's mobile device. Third-party soft token services from security providers such as VeriSign validates the user's identity thereby providing end-to-end security for mobile environments.

This two-factor approach significantly reduces the risk of "replay" attacks in which a hacker intercepts a user's credentials and then uses them in order to gain data access. Unless the hacker also steals the mobile device assigned to that user, simply replaying the user's credentials won't allow them access to protected data.

New, more flexible security tools are also available to help enterprise IT departments protect mobile data. For example, instead of relying on passwords to lock lost or stolen devices, IT departments now have the ability to remove data from lost or stolen devices remotely. For the first time users' personal—and thus unmanageable—mobile devices can be brought under centralized IT control. And while there is still no perfect mobile security solution, these remote control capabilities allow enterprises to better protect their mobile computing environments by striking the right balance between worker productivity and data security.

The availability of effective mobile security solutions may also break down barriers to the adoption of mobile computing in the financial services industry and other verticals that handle highly sensitive data. Many of these companies want the employee productivity gains provided by mobility, but consider the security risks too high. Now that these risks can be mitigated using a two-factor authentication process and remote IT management tools, companies that haven't been willing to take the plunge may finally be ready to.