iPhones Pose Conundrum for IT Departments

IT departments are in a quandary as iPhones and other mobile devices continue to replace the BlackBerry as the handheld device of choice.

The dilemma they face is that by allowing the devices to access business apps, they run the risk of running afoul of corporate IT and security policies.

“Corporate IT departments are usually regulated by a number of policies aimed at protecting sensitive information,” said Oleg Komissarov, vice-president of enterprise solutions at DataArt, which develops custom software for financial services firms.

“This can make them reluctant to implement extra services and information channels—email, for instance—that would extend any potential vulnerability.”

For a long time, this has meant that corporate IT departments had the final word on any new channels or devices within their environment.

“The situation has now shifted dramatically as the critical mass of users clamoring for new technology has reached a stage where it is impossible to ignore,” said Komissarov. “The main implication is that the previously closed corporate IT ecosystem has become more open and driven by consumers rather than management.”

The corporate concern for data and information security remains as users mix enterprise and personal data on their mobile devices. Business functionality available on mobile devices is often read-only or ‘subset of desktop’.

In combination with gaming and multimedia consumption, users’ attitudes towards mobile device privacy and information security may decrease, resulting in an increase of information leaks.

As a practical matter, these issues make things more expensive, as extra funds are needed to support added infrastructure and mobile data management for devices.

“With people growing more and more accustomed to stellar consumer-focused mobile user experience, their expectations and the related IT spend increase,” said Komissarov. “Overall, software quality standards are now dictated by mobile usage in a plethora of ways.”

The increased use of mobile apps translates into a greater reliance on cloud-based technologies.

“Any smart phone or tablet is an additional computer when it’s under corporate ownership or administration, essentially expanding a network beyond the traditional in-house infrastructure,” said Krassen Draganov, chief executive of Netage Solutions, a provider of front and middle office technology for the alternative assets industry.

The increased access that a modern mobile device provides and the higher margin of risk through loss—as people tend to carry mobiles around with them on person all the time— all add up to potential trouble for the employer.

“Mobile phones with access to cloud-based software that stores sensitive information needs to be configurable around security preferences and protocols,” said Draganov.

“Rather than storing a password on the phone, the feature should be disabled for traveling users. This enables a user to maintain access while minimizing the negative ramifications in the event of a loss.”