The MobilityHub
SECURING DATA & APPS.

John Edwards

Ensuring Encryption Really Works

John Edwards, Technology Journalist, 6/17/2013

Bio Email This Print Comment 10 comments

Rate It
👍 👎
50% 50%
Save It

Encryption is a powerful, essential mobile data security tool that many businesses either ignore or use incorrectly.

Many business managers fail to take advantage of encryption protection because as they begin investigating the technology, they quickly find themselves lost inside a murky world full of algorithms, ciphers, certificates, bit levels, and other important yet often arcane technologies and practices. Time-starved managers, confused by encryption terms and concepts, often throw up their hands in frustration and decide to move on to other projects, leaving mobile systems filled with important data that's left either poorly secured or completely vulnerable.

Fortunately, any business manager can successfully encrypt mobile devices without knowing very much about how the technology works. The best way to approach encryption is to view the technology as a lock that's designed to prevent outsiders from accessing confidential data. Most managers don't fully understand how an ordinary door lock functions, yet they know that using such a device helps keep unauthorized individuals out of buildings and offices. Data encryption can be viewed the same way.

Most mobile encryption products, such as Apple's FileVault for Mac notebooks, Microsoft's BitLocker for Windows notebooks, Apple's built-in iOS encryption, and Android's built-in encryption, can be used to lock down data without requiring users to understand the underlying technology.

While encryption software is easy to configure and deploy, it can't be regarded as a once-and-done task, since it's important to pay close attention to ongoing mobile data activity. For maximum protection, it's a good idea to select an encryption product that provides extensive reporting and auditing capabilities. These features let users check for compliance, receive system reports, and receive an audit trail. All of these capabilities help ensure that encrypted mobile data is always fully secure and that only authorized individuals have access to protected information.

Although managers prefer encryption software that's easy to deploy and maintain, it's also important to consider end-user needs. Many employees have little or no technical knowledge. Some may be downright technophobic. If an encryption program is overly complex, there's a risk that some users will avoid it, leaving their devices unprotected. A good encryption program offers centralized administration, making it virtually invisible to end users, yet still supplying the protection they need.

Simple oversights can derail the most carefully planned encryption strategy. Managers need to remember, for example, that plug-in memory cards, USB sticks, portable hard drives, and other attached storage devices also need to be encrypted. Another mistake is allowing users to send unencrypted data by email for use on their personal mobile computing devices, leaving the data vulnerable.

Related posts:

- Beyond Encryption
- Protecting Data at Rest
- 5 Tips to Secure Android for the Enterprise

Email This   Print   Comment