Enabling mobility within your organization: Re-evaluating your mobile security policy

Prepared by:

Soren Burkhart, *Principal,* McGladrey LLP
703.336.6400, soren.burkhart@mcgladrey.com

August 2013

As mobile devices expand their capabilities and become more functional, they have also become an integral part of how companies conduct daily business. Employees and customers now have an expectation of constant access to data and information, and the increased utilization of mobile devices is the best way to accomplish this goal. However, many companies are not familiar with the challenges that mobility presents and the consequences that can come with not having a true, disciplined policy in place.

A mobility strategy must be managed carefully to protect sensitive data and provide usage guidelines for employees. Vulnerabilities will never be completely eliminated, but they can be successfully mitigated if your policy is current and flexible enough to adjust to constantly emerging threats. The following are five common challenges that businesses face when implementing and executing a mobility policy.

BYOD: Bring your own device… or disaster?

Many companies have implemented a bring your own device (BYOD) policy, allowing employees to utilize personal mobile devices at work. This is seen as a win-win situation, reducing the cost of providing phones, and the employee has the freedom to choose any device and only carry one around.

The primary concern is that many companies don't implement a true mobile device management strategy, relying on what is in place for laptop computers. However, this policy simply does not cover the unique needs of mobile devices. Vulnerabilities often exist related to who is responsible for device replacement when a device is seized for discovery, what personal rights of privacy exist and what happens to data when employees leave.

Lack of mobile device security

Companies take varying approaches to secure end devices. Due to BYOD, businesses are forced to limit how much control they have over a device. Employees expect a certain degree of separation and privacy on their personal devices.

Unfortunately, the attack vector on exploiting mobile phones is greatly increasing. The return on investment is greater and the ability to access a mobile phone is much easier than infiltrating a work computer. The amount of information that is stored on a cellular device is also often more compromising and damaging: GPS data, SMS messages, emails, Web browser history, as well as VPN and personal wireless passwords.

Emerging mobile applications

In order to be perceived as progressive, many companies have deployed mobile applications. These apps commonly provide streamlined shopping experiences, increased access and enhanced information, generally making it easier to do business.

However, these applications are rife with security issues, with many of the same development concerns encountered with Web applications repeated with mobile devices. For example, some applications will encrypt the local authentication mechanism, but later pass an unencrypted session key that could be hijacked and used to impersonate the user.

Increasing cloud utilization

Difficulty in managing corporate networks has increased while pricing for offline storage has become more attractive. These factors have driven the increase in the utilization of the cloud for both computers and mobile devices. However, the growing amount of cloud services provides a wide range of security levels.

As the technology continues to develop, so do ways to intercept traffic to cloud servers that could lead to compromised data. Additionally, having all company documents in a cloud repository could create a single destination for hackers who are interested in accessing your data. It is difficult to enable data loss prevention measures when information can be leaked to multiple cloud services, such as iCloud, Google Docs, Amazon and others.

Users never learn

Unfortunately, no matter how hard companies try to educate users about security risks and technology responsibilities, training tends to wear off quickly. Employee behavior such as jailbreaking of phones is very common and is often performed without considering how devices become even more vulnerable and susceptible to attack. This behavior should be discouraged, due to the security loopholes it presents and lack of additional value it adds to the device.

Mobile security action items

In order to ensure that your mobile security plan is comprehensive, the following questions should be asked:

1. **Does your company have a BYOD policy? Are you aware of all the risks that may be associated with it?** The use of personal mobile devices can represent savings for your business and convenience for employees, but the risks involved must be understood and managed effectively.
2. **What types of mobile security are being implemented to secure mobile devices at your company?** Applications can be implemented and tailored to your unique needs to track activity and encourage proper usage and protect data.

3. **If you have mobile applications at your company, has anybody reviewed and checked them?**
   Many independent services and consultants are available that can analyze mobile apps to discover and remediate potentially dangerous vulnerabilities.
4. **What is your company doing about the cloud, and how has your data been secured?**
   The cloud is a cost-effective solution for data storage, but you must evaluate the security level of potential providers to ensure that your data is secure.
5. **How often do you train your users about security?**
   With the fluid nature of mobility threats, you must continually train your employees and reinforce the importance of adhering to the company strategy.

The use of mobile devices is surging and vast potential exists for enhancing business processes. Implementing an effective mobility strategy is a necessity to meet current demands and account for future growth. While the opportunities are plentiful, companies must be careful to understand the risks associated with mobile devices to secure critical data.

800.274.3978
www.mcgladrey.com