7 Critical Security Measures Every Business Must Put In Place NOW With Mobile Computing

If You Have Given Or Plan To Give Your Employees The Ability To Access Company Data And Systems With Mobile Devices – DON'T … Until You've Read This

Provided By: I-M Technology, LLC
Author: Stuart J. Bryan
131 Providence Street – Taftville – CT – 06380
www.i-mtechnology.com 860-237-8811

Mobile And Cloud Computing: Benefit Or Threat?

There's no doubt about it – the Internet and mobile and cloud computing have made our lives easier and our businesses more productive, cost-effective and competitive. But make no mistake about it: the Internet is also a breeding ground for thieves and predators, not to mention an enormous distraction and liability if not used properly. It is causing people to be casual, careless and flat-out stupid about their privacy in an increasingly litigious society where heavy fines and severe reputational damage can occur with one slipup – which is why you cannot be casual or careless about introducing it to your organization. You can't turn on the TV or read a newspaper without learning about the latest online data breach. And mobile devices are easily misplaced and stolen.

Because of all of this, if you are going to allow employees to use mobile devices – particularly personal mobile devices – to access, store and use company data, then it's critical that you have these 7 security measures in place.

1. **Implement a mobile device policy.** This is particularly important if your employees are using their own personal devices to access company e-mail and data. If that employee leaves, are you allowed to erase company data from their phone? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure YOUR information, or your clients' information, isn't compromised? Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured, but that doesn't mean an employee might not innocently "take work home." Whether or not it's company-owned device, you need to detail what an employee can and cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place. Require a signature acknowledging acceptance of the policy and your right to remove company data and access at will.

2. **Require STRONG passwords and passcodes to lock mobile devices.** Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode be entered will go a long way in preventing a stolen device from being compromised.

3. **Require all mobile devices be encrypted.** Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that unlocks (decrypts) the data. This can be invisible to the users

© 2015 I-M Technology, LLC – ALL RIGHTS RESERVED

and yet still protect company data.

4. **Implement remote wipe software for lost or stolen devices.** If you find a laptop was taken or a cell phone lost, "kill" or wipe software will allow you to disable the device and erase any and all sensitive data remotely.

5. **Backup remote devices.** If you implement Step 4, you'll need to have a backup of everything you're erasing. To that end, make sure you are backing up all MOBILE devices, including laptops, so you can quickly restore the data. Another option is only permit saving files, documents and photos (if relevant) to company cloud storage.

6. **Don't allow employees to download unauthorized software or files.** One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps. By implementing mobile device management users can even have authorized, safe applications automatically installed on their devices eliminating the possibility of downloading the wrong app.

7. **Keep your security software up-to-date.** Thousands of new threats are created daily, so it's critical that you're updating your mobile device's security settings frequently. As an employer, it's best to remotely monitor and manage your employees' devices to ensure they are being updated, backed up and secured.

Want Help In Implementing These 7 Essentials?

If you are concerned about employees and the dangers inherent in mobile and cloud computing, then call us about how we can implement a mobile and cloud security and monitoring system for your business.

Our process involves documenting all the mobile devices accessing your network, documenting what cloud applications your organization uses AND determining an appropriate backup for the data stored on third-party platforms. We'll also help you implement a mobile device policy, educate your employees on how to "stay safe" online and put critical security and backup services in place so you don't have to worry about data loss or unauthorized access to your company's network.

To- request a FREE, no-obligation Mobile And Cloud Security Assessment, call us at 860-237-881 or email me at sbryan@i-mtechnology.com.

© 2015 I-M Technology, LLC – ALL RIGHTS RESERVED