Courtesy of
TriSure Corporation

CYBERRISKS&LIABILITIES_

Securing Your Company's Mobile Devices

Because of the convenience they offer, smartphones and tablet devices have become a ubiquitous presence in the modern business world. As usage soars, it becomes increasingly important to take steps to protect your company from mobile threats, both new and old.

The need for proper phone security is no different from the need for a well-protected computer network. According to computer security software company McAfee, cyber attacks on mobile devices increased by almost 600 percent from 2011 to 2012—and experts expect that number to increase again in 2013.

Gone are the days when the most sensitive information on an employee's phone was contact names and phone numbers. Now a smartphone or tablet can be used to gain access to anything from emails to stored passwords to proprietary company data. Depending on how your organization uses such devices, unauthorized access to the information on a smartphone or tablet could be just as damaging as a data breach involving a more traditional computer system.

Lost or Stolen Devices
Because of their size and the nature of their use, mobile devices are particularly susceptible to being lost or stolen. According to a 2012 study by the Ponemon Institute, nearly 40 percent of organizations experienced a data breach as a result of a lost or stolen mobile device. Since most devices automatically store passwords in their memory to keep users logged in to email and other applications, gaining physical possession of the device is one of the easiest ways for unauthorized users to access private information.

To prevent someone from accessing a lost or stolen device, the phone or tablet should be locked with a password or PIN. The password should be time sensitive, automatically locking the phone out after a short period of inactivity. Most devices come with such security features built in. Depending on your cellphone provider, there are also services that allow you to remotely erase or lock down a device if it is lost or stolen. Similarly, it is possible to program a mobile device to erase all of its stored data after a certain number of login failures.

Malicious Attacks
Mobile devices have the potential to be just as susceptible to malware and viruses as computers, yet many businesses don't consider instituting the same type of safeguards. Less than 20 percent of mobile devices have antivirus software installed, which is practically an open invitation to a thief or hacker to pillage whatever information they want from an unprotected device. Furthermore, it doesn't matter what operating system the devices use, whether it be Android, Apple's iOS, Blackberry or Windows Mobile—all are vulnerable to attacks.

As reliance on these devices continues to grow, so will their attractiveness as potential targets. Third-party applications (apps) are especially threatening as a way for malware to install itself onto a device. These apps can then purchase and install additional apps onto the phone without the user's permission. Employees should never install unauthorized apps to their company devices. Apps should only be installed directly from trusted sources.

Hackers can use "ransomware" to restrict a user's access to their device's data, contacts, etc., and then demand a ransom to get it back. Even if the user pays the ransom, there is no guarantee that they will get the data back. Employees should know not to ever pay the ransom if this type of software finds its way onto a company device.

TRISURE

A big difference between mobile devices and laptops and other computers is the ability to accept open Wi-Fi and Bluetooth signals without the user knowing. Hackers can take advantage of this by luring devices to accept connections to a nearby malicious device. Once the device is connected, the hacker can steal information at will. To prevent this, make sure all mobile devices are set to reject open connections without user permission.

Preventive Measures
While the current mobile device security landscape may look bleak, there are plenty of ways to be proactive about keeping company devices safe from threats.

1. *Establish a Mobile Device Policy*

Before issuing smartphones or tablets to your employees, establish a device usage policy. Provide clear rules about what constitutes acceptable use as well as what actions will be taken if employees violate the policy. It is important that employees understand the security risks inherent to smartphone use and how they can mitigate those risks. Well informed, responsible users are your first line of defense against cyber attacks.

2. *Establish a Bring Your Own Device (BYOD) Policy*

If you allow employees to use their personal devices for company business, make sure you have a formal BYOD policy in place. Your BYOD security plan should also include the following:

- Installing remote wiping software on any personal device used to store or access company data.
- Educating and training employees on how to safeguard company data when they access it from their own devices.
- Informing employees about the exact protocol they must follow if their device is lost or stolen.

3. *Keep the devices updated with the most current software and antivirus programs.*

Software updates to mobile devices often include patches for various security holes, so it's best practice to install the updates as soon as they're available.

There are many options to choose from when it comes to antivirus software for mobile devices, so it comes down to preference. Some are free to use, while others charge a monthly or annual fee and often come with better support. In addition to antivirus support, many of these programs will monitor SMS, MMS and call logs for suspicious activity and use blacklists to prevent users from installing known malware to the device.

4. *Backup device content on a regular basis.*

Just like your computer data should be backed up regularly, so should the data on your company's mobile devices. If a device is lost or stolen, you'll have peace of mind knowing your valuable data is safe.

5. *Choose passwords carefully.*

The average Internet user has about 25 accounts to maintain and an average of 6.5 different passwords to protect them, according to a recent Microsoft study. Obviously, this lack of security awareness is what hackers count on to steal data. Use the following tips to ensure your mobile device passwords are easy to remember and hard to guess:

- Require employees to change the device's login password every 90 days.
- Passwords should be at least eight characters long and include uppercase letters and special characters, such as asterisks, ampersands and pound signs.
- Don't use names of spouses, children or pets in the password. A hacker can spend just a couple minutes on a social media site to figure out this information.

TriSure Corporation has worked with industry experts to craft sample mobile device policies that can be further customized to fit your unique business needs. Contact us today to obtain a copy of the policy.