GENSCORP IT
INFORMATION TECHNOLOGY SOLUTIONS

Mobile Device Security

genscorp.com

Employees are bringing their own devices to their workplaces more frequently and forcing business owners to consider mobile device security practices within their organization. From smart phones, tablets, USB thumb drives, to laptop computers – mobile devices take on many shapes and forms but all introduce new risks to the privacy and security of your business data.

Mobile Device Risks to Consider

Today's mobile devices can store a large amount of data. Unfortunately, they are also small in size and easily portable and the data stored on a mobile device is rarely protected. If precautions are not taken to protect the data on a mobile device that gets stolen or lost,

unauthorized individuals could suddenly have access to private information which may lead to a network security breach, compliance issues, and a variety of other technical nightmares! Of laptops that are stolen, more than 50% result in a data breach.

"If precautions are not taken to protect the data on a mobile device that gets stolen or lost, unauthorized individuals could suddenly have access to private information..."

Even if the information is not physically stored on a mobile device, the fact that the device has access to the network or other services can enable unauthorized individuals to access non-public data including the company email, applications, or Virtual Private Networks.

Mobile Device Benefits

An iPass survey of 1,100 mobile workers around the world indicates that workers using their mobile devices for personal and work related tasks put in 240 more hours than workers who do not use mobile devices. Cisco reports that their company-wide, any-device policy results in an increase of 30 minutes of productivity per employee per day. The benefits of allowing mobile devices in the workplace make the risks worthwhile, but it is important to put appropriate mobile device security policies and systems in place to reduce those risks.

Mobile Device Security Guidelines

The following guidelines will ensure the protection of privacy and data in the event a mobile device is stolen, lost, or compromised in some way.

• Mobile devices should be labeled with name and contact information in case it is lost. This will allow honest individuals to return the device to the owner even if the battery is dead and the unit cannot be powered on to determine who it belongs to.

- Passwords should be in place to limit access to the device.

- Phones and tablets and other mobile devices should automatically lock themselves if they are not in use after a certain period of time. Unlocking should require the password.

- Update all software, applications, and the mobile device operating system regularly to ensure the device is
protected from attacks and vulnerabilities.

- Create a mobile device management environment to configure and maintain security and privacy settings across all devices on the network.

- If using an iPhone, iPad, or iPod, enroll in the Find my iphone or equivalent service to put GPS into use if the device is lost or stolen.

- If a mobile device supports hardware and storage encryption, set up the service so data can be deleted remotely in the event the mobile device is lost or stolen.

- Portable storage devices (such as removable hard drives and USB memory sticks, etc) should be encrypted in case they are lost or stolen.

"Create a mobile device management environment to configure and maintain security and privacy settings across all devices on the network."

GENSCORP IT
INFORMATION TECHNOLOGY SOLUTIONS

233 1st ST. W. North Vancouver
Suite 350 BC Canada, V7M 1B3
Office: (888) 299-3331
Fax: (888) 220-7317