Law Firms and Mobility

To meet client demands, people need to connect to data at any time and from multiple means. A variety of mobile devices, which include laptops, tablets, and smartphones, are being used to connect to firm data. Some of these devices are provided by the firm, while others are owned by firm employees and brought into the workplace, a practice known as BYOD: Bring Your Own Device. These devices do not always have the necessary security measures in place to protect the firm and are therefore becoming a target of those trying to gain unauthorized access to firm and client information.

Mobile Devices and Risk

Because mobile devices often include cameras, recording capabilities, and Internet access, they provide a number of potential information sources for hackers. In addition, mobile devices are capable of storing large amounts of client and firm data. Because people are using mobile devices like personal computers, the devices are as vulnerable to web-based attacks as desktop users.

* When files are opened and viewed on mobile devices, many devices store a copy of the document on the device. The document may contain protected or confidential information.
* Editing or sending documents via mobile devices can raise concerns about metadata since the typical cleaning tools used on desktops are sometimes bypassed.

Best Practices for Mobile Device Use

* Learn and follow firm policies on mobile devices. Follow guidelines for device passwords, encryption of data, and security software.
* Report loss or theft as soon as possible so steps can begin to secure the device and wipe the data.
* Use strong passwords, longer than 4 digits, on devices. Avoid using proper names, initials, or birthdates.
* Be conscientious of your surroundings and be mindful of what is visible on screens and who can see passwords or data entered into devices.
* To decrease the risk of theft, avoid using mobile devices in highly congested areas, such as busy streets, transit stations, or on crowded trains.
* Avoid clicking unfamiliar links, scanning QR Codes of unfamiliar sources, or opening text messages from unknown senders.
* Make sure current versions of the operating system and applications are installed on mobile devices to reduce opportunities for security breaches. Follow firm guidelines in the installation and use of device applications.