MOBILE DEVICE SECURITY

By Rebecca Sattin
CIO, World Software Corporation

While mobile devices have been around for many years, it is only more recently that the need to secure them has come to the forefront.

In the beginning, there was the BlackBerry®. With the emergence of their devices that looked like oversized pagers in 1999, they brought 24x7 access to email into the hands of attorneys and IT staff. With the advent of the BlackBerry Enterprise Server, they quickly became ubiquitous in the legal market as they enhanced the business person's ability to support clients even while away from the office.

While many other manufacturers came out with devices for business people, it was in 2007 when Apple® changed the game with their introduction of the iPhone®. They combined their consumer iPod® device with cellular phone technology and, by doing so, created a conundrum in the business world. This device forever changed expectations of what a mobile device should be and everyone wanted one. A new word was introduced into the lexicon: consumerization.

This new age brought great challenges to legal IT departments. In the past, legal staff were more skilled in the use of technology than attorneys. With the advent of new consumer technology with price points that made it more available to attorneys than staff, the tables began to turn. Where once we had to struggle to persuade attorneys to use new technology, they were now coming to IT demanding the support of these new devices. The introduction of consumer products and the demand for these products among attorneys compelled IT to face the conflicts between convenience and security. Those of us in the legal IT world had to weigh the demands made by attorneys to support the device against our concerns over security. The iPhone® was clearly a consumer device, but we were asked to adapt it for business use.

It wasn't until security concerns came to the forefront with FBI warnings in 2009 and 2012 that law firms began to focus on developing more robust mobile device policies to address the need to keep firm and client data secure. The fact that firm and personal information were comingled on one device added a layer of complexity to the situation. Simultaneously, litigation support practices evolved to accommodate the issues surrounding discoverability of mobile device data. Policies ranged from simply requiring a password on the device to requiring agreement to have the device wiped upon leaving the firm or upon report of loss.

Here are just some of the questions firms considered before creating policies or seeking out software to manage the devices:

- Who will pay for the device?
- Who will pay for the service?
- Who will be allowed to have a mobile device connected to the system?
- Will those who have mobile devices need other functionality besides email, calendar and contacts?
- Are there other apps available for business functions that will be required?
- What will the practice be when someone leaves the firm?
- Will the device be used for only business?
- Will the law firm allow or prohibit a "bring your own device" (BYOD) policy?
- How many types of devices will be supported?

Additionally, depending on the software used to manage the devices, firms will need to assess their risk and exposure so that they can prioritize their needs for the following features:

- Remotely wipe lost or stolen devices
- Track devices via GPS
- Limit connection to wireless networks
- Limit functionality based on GPS information
- Limit applications allowed
- Push firm applications to the device
- Push application configurations to the device
- Enforce password requirements
- Enforce device lock requirements
- Remote configuration of the device
- Block information from appearing while the screen is locked

Many solutions are now available to help IT Departments manage devices once decisions have been made about the above needs and functionality. Depending on the size of the firm and IT department, there are hosted solutions available.

The approach to the issues above will also determine whether or not a containerized solution is warranted. Containerized solutions create a secure, encrypted partition on the device that often requires an additional password for access to firm information. They allow a single device to be used for both business and personal needs while maintaining the necessary controls required to secure the firm's data. With a containerized solution, firm data and personal data can coexist on a device and, depending on requirements, devices can be configured so that no interaction between firm and personal data is possible. Some lawyers want the freedom to use their own mobile device instead of one issued by their law firm. From a security standpoint, a containerized solution will satisfy the need to protect firm and client data while allowing attorneys freedom of choice.

While many threats to security still exist, there are now more options than ever before for safeguarding data on mobile devices. Many legal software vendors provide mobile device apps that attorneys can use to be more productive while out of the office. Many of the Mobile Device Management solutions support the interaction, containerization or distribution of those apps within their products. The compatibility and availability of other business apps should be considered when choosing a solution. The IT staff can take the following steps to enhance security:

- Fully encrypt all mobile devices used by the firm's attorneys
- Encrypt data before it is sent to the cloud
- Stay up to date with vendor releases and patches
- Discourage the use of thumb drives for transferring data from laptops to other devices
- Conduct an annual vulnerability assessment

Mobile Device Management has come a long way in 15 years and mobile device security has matured to become more reliable than ever. Robust safety measures and an increase in the availability of legal apps make it possible for attorneys to access firm data from their mobile devices, enabling them to be productive anywhere.

Rebecca is CIO of World Software Corporation. She was formerly at Mitchell Silberberg & Knupp LLP for 18 years, where she was Director of Information Technology. She has more than 20 years of experience in the area of law firm technology. She spoke on "Talking Technology to Lawyers" at Legal Tech Los Angeles 2012 and has spoken on various topics at many of the last several International Legal Technology Association (ILTA) conferences. She spoke at the Good Exchange conference in New York in 2014 on mobile device management. She has also served on the advisory board for LA City College's Computer Technology department. Rebecca is a graduate of Washington University in St. Louis.

LEGAL TECHNOLOGY SPECIAL ADVERTISING SECTION 2015