APRIL 11, 2016

Legaltech® news ONLINE

An ALM Publication

Securing Your Device: BYOD Platforms for Legal

The evolution of mobile management and what it means for security, privacy, and the future of mobile lawyering.

BY RICCI DIPSHAN

©iStock.com/derrrek

As the Information Age evolved, the data it transported took on entirely new dimensions—no longer static or tied down, but a living, breathing and above all, moving, entity. And like a young child just learning how to walk, it had to be protected.

But instead, it took off running, and years were spent playing catch up. Until one industry finally sprinted ahead, and in doing so, pulled all those struggling behind up to frontlines.

This is, in a sense, how the legal industry came to the forefront of the effort to secure mobile data. Not out of its own volition, but as a part of the domino effect of a fundamental shift in how businesses handle mobile data.

"The financial and banking industries were the first to have to crack down on mobile data security—and regulators forced banks to make sure that their data was to be protected wherever it was in the same manner they would protect it in house," explains Neil Watkins, vice president of security, risk, and compliance at Epiq Systems.

It was the financial and banking sector, he adds, that forced many legal firms and companies into an "overnight maturation" on mobile data security. And despite its lateness to the cause, "the legal industry is probably the most responsive industry on the planet when it comes to changes."

The industry was, after all, a quick adopter of the bring-your-own-device (BYOD) movement, when smartphones and tablets first appeared. "When BYOD had its heyday, it was productivity at all costs," says Watkins.

"But then they said, 'Look we really can't go this way. We have to provide gold plate protection services to all our data as if it were in our core systems.'"

MDM: Lock, Control, Contain

And so the field of enterprise mobility management (EMM) was born, and with it the first mobile data protection software, mobile device management (MDM).

The principle behind MDM, explains Watkins, was making a "mobile device become a container in space. ... Companies were saying, 'We are going to solve this problem by creating a corporate container on that device or making the whole phone a container.'"

To Philip Gordon, shareholder and chair of the privacy and background checks practice at Littler Mendelson, this "container" is essential in being able to manage, safeguard, and keep track of a company's data. "[MDM is] the only way the company is going to have an inventory of all the devices that are accessing its network. And it permits the employer to push security controls to the user's device, including key information protection like password protection, encryption and remote wipe ability."

Chris Hazelton, director of product marketing and strategy at Apperian, explains that MDM platforms are easily created by using APIs that Google or Apple published for corporate use, which also allow the installation of "VPNs for the entire device as well as corporate email and Wi-Fi access points."

MDM's safeguards, however, can at times come across as an overbearing, heavy-handed solution for security.

"Some employees are concerned when they read a BYOD policy, and the employer is telling them that they have the ability to wipe their entire device, and they're going to install encryption and password protection and lockdown after periods of inactivity. There are some employees that don't want to permit the employers to have that level of control over their personal device," cautions Gordon.

But many get around this burden by limiting MDM to a folder, "and if we have to issue a remote wipe command, we can wipe only the stuff in the container," he adds.

While seemingly airtight from an IT perspective, MDM protections, however, still depend on employee cooperation. "The blind spot of that type of approach is that it assumes employees will abide by the rules and store all corporate data only in the containers. I think if employees are planning to misappropriate a company's trade secrets, that's the last place an employee is going to store them before leaving."

MAM: There's a (Private) App for That

To some, MDM can feel like a clunky and outdated solution to data security, especially in its emphasis solely on a user's particular phone or tablet. So developers came up with a more agile solution that "is much more focused on the data and the application than the device," says Hazelton.

Mobile application management (MAM), he explains, is about "delivering applications through the device—and it doesn't matter who owns the device or if it has MDM or not. [With MAM], I'm able to essentiallly create a private app store, and any app that comes out of that app store can be managed directly."

MAM can also mimic and go beyond most of the same protections as MDM, for example, by requiring "that the device has encryption or a password" to download its app store or "protect content on an application, where users can't copy the content from that application and paste it into twitter or Gmail," says Hazelton.

The platform, he adds, gives employers less control over a user's phone or table, makes it easier to protect the mobile data of clients or part-time, temporary employees on

unsanctioned devices, and gives a company the opportunity to create and distribute proprietary apps to their workforce—a market that is exploding in the legal world and beyond.

"MAM also need not replace MDM—despite their different approaches, the platforms' protections are not mutually exclusive," Hazelton explains.

"MDM is driven by your password, passcode ... once [hackers] break the password, they decrypt the password, they have access to the entire device—that's one threshold," he adds. "If you want to have another threshold, which will have a separate layer of encryption ... those [MAM] applications will have separate layers of encryption."

VMI: What's Here Never Stays

With the launch of MAM, the EMM's focus broadened to manage the use of multiple devices among employees and clients. But for some companies, this was only the first step in creating ever more protected accessibility.

Enter virtual mobile infrastructure (VMI), which Gopal Jayaraman, CEO of Sierraware, argues surpasses other EMM security by completely keeping all data and company software off of a device. "With VMI, you don't have to worry about what happens when the phone is stolen because there is no data on the phone. Everything is installed in a server and people just access it remotely. ... VMI solves the problem much simpler and much more efficiently you don't have the worry about the phone and the data."

What's more, "MDM limits you to access that data from one particular device. ... You cannot install MDM on all devices you have at phone, but any device in any location can link up to a VMI server," Jayaraman adds.

Although VMI is billed as the evolution of virtual desktop software, it is not all that new—its core networking technology has been around for at least decades. But what makes modern VMI different, says Jayaraman, is mobile application virtualization. Some VMI infrastructures run "an instance of an operating system for each user ... so each Android OS instance may require on 1 GB of RAM," making it sluggish and difficult to use.

"But you can virtualize—you can get up to more than 200 times the space," he explains. "That is our biggest advantage, and why we can deploy much wider."

This also means that users "can continue to use the same apps they were using before, and with the same IT. The user's experience is exactly the same, but data is never stored on the phone."

Yet like every platform, VMI is not without its shortcomings. "In reality, the major drawback is that it is totally network dependent. No network, no apps. So it's not like being unable to find Wi-Fi and you can't get new emails; instead, you can't even look at anything on the device because nothing is cached on the device," explains Hazelton.

Whether this modernized networking technology, an agile app-centric management software, or a traditional device-focused digital container will rule the future of the legal industry's mobile security is anyone's guess. But like many things in legal tech, as the technology consolidates and evolves, it may become a matter of choice and preference—a much needed luxury in an industry that only recently caught up to the perils of unfettered mobile information.