Why RIAs Are Better Off With 'Dumbed Down' Smart Devices

February 18, 2016

Smart mobile devices have revolutionized the wealth management business, transforming the way advisors connect with clients and manage day-to-day firm operations. Today it is more common than not for registered investment advisors (RIAs) to use their mobile phones, tablets and other devices like computers. Without the right security in place, advisors who relish their "office anywhere" mobile environment may pay a hefty price for this convenience.

Advisors who would never think of using their CRM or other core business applications via an unprotected computer in the office balk when the talk turns to protecting mobile devices that access the same applications. The rationale for resistance tends to be that securing a mobile device will compromise the convenience of the device by slowing down access, which can be frustrating.

Web-based applications may help the business of wealth management be more efficient, but they are not secure. This means that the RIA is responsible for ensuring security on every device through which the application is accessed—desktop computers, laptops, smart phones, tablets, whatever. In the wrong hands, an unsecure tablet or smart phone has the potential to be the gateway into the financial lives of all the RIA's clients.

Though mobile device security is a must-have, advisors have a couple of options on how to go about protecting firm and client data.

Dumb-Down The Devices

Mobile phones in particular are easy to lose, consequently, they are most likely to get hacked. In fact, Consumer Reports found that 3.1 million people had smartphones stolen in 2013 and an additional 1.4 million phones were lost and never recovered. That is why simply having the mobile phone password protected is not enough. Loaded up with the firm's web-based applications, the lost device is a potential goldmine for cybertheives.

It can be extremely difficult for the RIA to protect every mobile device used to access the firm's data. Consider the advisor who borrows their spouse's mobile phone just to check on a client account because their device is out of juice. And then there's the employee who is at home unexpectedly but is logging onto web-based applications from their personal laptop. In each of these instances, the user may be accessing firm data from an unprotected and unsecure device.

The RIA's best safeguard is to remove all the firm's web-based applications from all mobile devices. This means that the devices have only one application—the one that gets the user to

the firm’s protected smart platform. The mobile device user goes through a secure connection protected with multi-factor authentication to log into the RIA’s secure platform. Once on the platform, they can get to any application they need through a centrally managed password vault and do not need to know the centralized credentials to do so.

By keeping their devices as dumb as possible, RIAs force staff to use the secured smart platform and protect themselves in the event devices are lost or stolen. Think of the difference between a remote control and a television set. The television set has the channels for the programs you want. The remote control allows you to operate the television set to get to those channels and programs, but you can’t use the remote control without access to a signal from the television. In other words, dumbed-down mobile devices (the “remote controls”) do not provide advisors and employees access to the needed applications (“channels and programs”) unless they are logged into the firm’s smart platform (“the television set”).