A Remote World: Cybersecurity And Your Tech Stack

August 6, 2020

The Covid-19 pandemic has given advisors greater appreciation of their need to be flexible and accessible in their working arrangements—and at the same time, for their technology to be safe and secure. We are going to be shifting to a “new normal.” That might mean gearing up for life back at the office, or it might mean working from home for the foreseeable future.

In any case, the way RIAs manage their tech stack security must be consistent. By now, advisors know they must apply the same rigorous policies and protocols they used at the office to the remote computer networks they’re tapping from home. Cybercriminals didn’t go on hiatus when the coronavirus struck; in fact, there has been a dramatic uptick in phishing e-mail attempts against RIAs since March, when the pandemic forced many workers to go home.

The pandemic has shown RIAs that they need a way to operate using the end devices and power available at their homes. What may come as a surprise—and perhaps a relief—to RIAs is that there is quite a bit of flexibility in how their cybersecurity can be achieved remotely.

It starts by thinking through their firms’ tech stacks and taking an umbrella approach to bringing users and devices into the “social pod.” This popular terminology describes a closed loop of small groups that have agreed to interact exclusively during the pandemic.

Until recently, most RIAs typically managed their technology in one of two ways—either through a virtual cloud environment or through individual workstations. Each model has its own pros and cons when it comes to data security, speed and flexibility. For instance, bandwidth and speed issues can make collaboration on documents and in-office workstreams difficult to maintain in many home-based work environments. It may be easy to say that the remote log-in or virtual cloud environment is best, but it might not be practical for everyone at home since staff members likely have different degrees of bandwidth and Wi-Fi capabilities.

Enter The Hybrid Tech Environment

But there’s a third way—a hybrid approach—that offers the best of both of worlds. Here, advisors and firm staff operate off of a combination of centralized and decentralized environments simultaneously, which can be critical in remote work circumstances where bandwidth capacity and devices may be an issue.

Say an RIA uses a fintech or custodian application using a secure Citrix connection, which requires a known computer or IP address to access. Using a centralized, highly secure

environment with special connectivity solves for this. But it also requires a considerable amount of bandwidth.

The hybrid approach allows advisors and their teams to collaborate using their tools and desktop applications in combination outside of the firm’s centralized private cloud, and also maintain a highly secure and compliant environment without sacrificing data transmission speed or quality.

Though “going hybrid” may make the most sense, it does not mean firms can simply put a software agent—or access control application—on any device they choose and in an instant make all access to information, data and applications secure.

In fact, the hybrid approach requires a high level of management to secure the firm’s data and devices from potential breaches and to remain compliant. This means every single end device being used by advisors and staff must be known and encrypted and meet compliance policies.