Vetting Vendors? Ask these Questions

December 27, 2017

In the RIA community, we can certainly learn from the Uber breach.

Whether you’re evaluating a third-party provider, it’s not enough to hear, “The data is encrypted.”

Vulnerability can start long before the data is encrypted.

Every portfolio management solution, rebalancing CRM, or backup company will tell you that their data is encrypted. But what happened before the data got encrypted? Every program that is written must be executed under authority to access data…otherwise the program can’t do anything. So it doesn’t matter if the data is encrypted when someone initially had administrative rights—because admin rights provide access to everything.

Choose your vendors wisely

It’s your job to screen your vendors, because when a third-party vendor has an issue—it’s ultimately your issue. Do your due diligence. Start at the very beginning. When vetting any kind of third-party vendor—consider/ask the following:

- How was security managed during the development of this product?
- Who had/has access to the source code?
- Who had/has admin access and how is that kept secure?
- How did you ensure that credentials were not encoded or shared accidently?

It happens all the time. When auditing source code, major holes are often found that leave back doors for programmers. Without strict controls, you don’t know what a programmer has put in the code or shared. This is why, when any kind of development is done—auditing procedures must start at the beginning.

If Uber made this error, there are countless others who’ve done the same—because security wasn’t architected properly from the beginning.

Need help vetting vendors? At RSS, we will help you make secure decisions. Let’s talk.