THE FUTURE OF BANKING

Effects of Data Breaches on Vendor Management

"In the past we could point to our service provider and say 'it's stored with ABC Company.' In today's climate, this will create an audit deficiency; you need to know where it is physically stored."

— MARK C. DITTMAN, IBT CEO

As data breaches continue to impact consumers, security and storage of data has come under increased scrutiny during internal and external audits. This will initially impact your vendor management risk assessment and policy. You need to make sure that your risk assessment addresses breach of your NPI (non-public information) data with and without notification by your vendor. Be aware, if a third party is accessing your data from your core provider, you may need to know if this is done in batch or real time, as each may carry a different set of risks.

Not all NPI data is secured the same way. For example, debit card data normally falls under PCI audit. With PCI compliance there are very good controls around how the data is stored and managed in the banking sector. However NPI data related to loan and deposit document images falls under the controls of an SSAE16 audit and the control requirements are different. NPI data that is included in PCI audit must be encrypted while at rest (stored) and in flight (during processing). NPI data part of an SSAE16 does not require encryption at rest, but requires encryption in flight.

So now that you know how your data is stored and transmitted, you need to know where your data is, what systems have access to that data, and where those systems are housed. In the past we could point to our service provider and say "it's stored with ABC Company." In today's climate, this will create an audit deficiency; you need to know where it is physically stored.

That brings us to the cloud and how that is used to manage your NPI data. With so many applications moving to the cloud, we need to have a better understanding of what it means. The cloud requires us to understand how a specific vendor's solution utilizes the cloud. Is the application being hosted on a virtual machine in the cloud (SaaS), or is the application operating as platform as a service (PaaS). There are others, but these are the most common. With a SaaS application, we can think in terms of a physical server at one location, but PaaS applications can use multiple physical servers in multiple physical locations. Keep in mind, newer platforms tend to take advantage of the PaaS design.

As you have the opportunity to select vendors, make sure the image data is encrypted at rest, protecting your bank, your clients, and your vendor. When you start examining how your application is processed in the cloud, make sure your vendor understands the different methods and which methods apply to each application you have from them. Ideally, your vendor should include data mapping as part of their own compliance. Otherwise, you will have challenges determining where your data is housed, secured, and how to mitigate your risk.

IBT is a true partner that strengthens relationships and enhances customer retention. For more information, visit IBTapps.com.

IBT®

1101 Arrow Point Dr. #305, Cedar Park, TX 78613
512.616.100 | sales@IBTapps.com | IBTapps.com