It's All About Data Security – Or Lack Of

John H. Taylor

December 2018

In the span of just one month we have learned of two massive data security breaches at Starwood and Quora affecting 600,000,000 or more individuals – many of whom are own staff members:

https://www.nbcnews.com/tech/security/marriott-says-data-breach-compromised-info-500-million-guests-n942041

https://www.nytimes.com/2018/12/04/technology/quora-hack-data-breach.html

Are you next? Based on our visits to client sites around the country, you are probably in decent shape *as long as your data is under your control*. FERPA, HIPAA, PCI DSS, etc. have been around long enough that we have had the lid clamped down tightly when it comes to our own internal systems.

But what happens when "your" data is no longer under **your** control? As more institutions evaluate SaaS and PaaS solutions for their advancement CRM and related fundraising activities, we must acknowledge that we are not always going to be in control of our precious data assets. We must rely on others to ensure our data are properly safeguarded when entrusted in their care.

The good news is that every primary SaaS or PaaS product in play for our use these days are very public regarding what measures they have taken to protect data. And our own internal security experts very likely have requirements we must check on before acquiring such a solution. Stanford University, like many others, have websites devoted to this topic:

https://uit.stanford.edu/guide/securitystandards/saas_paas

But what should we look for? When it comes to SaaS we can expect reliable providers to be fully credentialed. PivotPoint Security lists the most common security accreditations:

https://www.pivotpointsecurity.com/blog/security-accreditations-for-saas-providers/

But what about working with service providers who do not store our data – but use it (wealth screening, biographical append services, employer locator vendors, etc.)? Look for similar credentials. The main wealth screening vendors have been SOC 2 compliant for a long time. The other forms of append services may not necessarily need to subscribe to as strict a protocol. On the other hand, if they are not utilizing security protocol such as encrypted file transfers and FTP transmission facilities, you might want to dig deeper into what safeguards they are taking.

What's important in today's fundraising environment is knowing what happens to your data when it is no longer "your data." You do not want to read about yourself on the next security breach webcast!