Sarah MacEachern - Sun, 10/20/2013 - 00:00

Just a decade ago, most data lived in spreadsheets and databases close to home, sometimes right on our desk. IT departments guarded access. The greatest risk to our data was loss through system failure, so full data backups were the rule. Occasionally we would hear of someone's computers being "hacked," but it was not a common occurrence.

What happened? Offsite solutions, born in part by the disaster recovery push after 9/11 and the technology that sprang up around it. Hosted or cloud storage became cheap and offered freedom from fears of data loss due to hard drive crashes or mysterious server malfunctions – and also meant greater access to data. Where memory and notes scribbled in tattered files once guided donor cultivation efforts, a few taps on our phones or tablets now reveals up-to-the-minute information and analysis. However, with great (technological) power comes the great responsibility of data security – your data and personal data your donors have entrusted to you.

We read stories about the latest data breach. Who's to say your data isn't next - or, worse, data entrusted to you by your donors? If you're in the information services field like PG Calc, you really, really hope it's not data that has been entrusted by a donor to your client who has entrusted it to you. Fortunately, there are data security measures to make sure everyone's information is only available to the people who are supposed to see it. In fact, you may be legally bound to put those measures into place!

Massachusetts paved the way in 2010 with a requirement that any companies or persons who store or use personal information (PI) about a Massachusetts resident develop and maintain a Written Information Security Plan (WISP). Similar regulations have sprung up around the country, and that is a good thing. The new rules don't mandate the same methods or implementation (except in regulated industries like financial services), but they do insist that businesses and organizations think about and document the steps they are taking regarding data security. It can be difficult to write down your policies and implement processes to enforce those policies consistently, but it's time well spent.

Here are some of the mission-critical areas we include in our WISP:

Ongoing administration of information security program
Security awareness training
Program compliance safeguards
Effective, mandatory password policies
Company-wide rules on handling of personal information
Universal e-mail encryption
Record retention policies
Consistent controls and monitoring of third party service providers
Documented procedures for risk assessment and incident management

Some of these policies and guidelines include state or federally mandated components. In these cases our WISP outlines how we go beyond those required elements to achieve practical, measurable, and effective practices we can implement and follow every day. Adhering to the rules part of our company culture and violations can result in dismissal. Anything less makes compliance difficult or impossible. At PG Calc, even our 10- and 20-year veterans (and we've got a lot of them!) undergo annual refresher training to stay current. We all understand the damage that data security lapses can cause to our clients and our company, and that our WISP helps protect us against that.

The items above apply to all the information we handle regardless of whose it is. Even higher levels of protection are in place for the highly sensitive information for users of *GiftWrap* and our other hosted products. These include:

Transparent Data Encryption (for databases at rest)
Firewalls for additional barriers to access
Separation of powers for servers
DMZs (not just the one separating the Koreas)
Physical / premises security including biometric scanning
Redundant Power and Internet supplies

It's true that a really good hacker can probably bypass these security measures, or anyone's. It's also true that a really good car thief can steal your car no matter what you do to secure it. Effective data security is all about making the casual thief look for an easier target – the equivalent of remembering to always lock your car and keep valuables out of sight.

Print

Categories

PG Calc Featured Articles