Valley Nonprofits Should Beef Up Cybersecurity

BY CARRIE COLLINS-FADELL
CONTRIBUTING WRITER
AUG 23, 2019 | *PHOENIX BUSINESS JOURNAL*

While there are many ways the nonprofit and for-profit sectors are different, when it comes to the safety of their online footprint, it appears this is one area in which they have more in common than not.

As outlined in the July 5 Phoenix Business Journal cover story, "Small Isn't Safe," any business, no matter the size or market, presents a ripe target for a cyberattack, whether it be a monetary or technology theft or a data breach. And this includes the nonprofit sector.

Nonprofits and religious entities tend to be as much a target as for-profit sites. In some cases, a well-vested list of contacts and donors is more valuable to hackers than the immediate monetary gain from ransom or theft.

According to SiteLock, small business cybersecurity threats have become so common that the average website was attacked 44 times a day during the fourth quarter of 2017. Every nonprofit that has a website and uses it as an electronic business card and the face of the company should have multiple layers of protection.

These can be simple things like being mindful of the construction of your website and the platform it is built on, hosting provider, and password security protocols. Scheduling routine password changes and the use of encrypted password generators to allow for nondescript passwords that are more difficult to hack are all simple steps nonprofits can take in addition to working with area professionals. Small nonprofits can enhance web security with user-friendly interfaces, allowing key staff and board members to be part of the protection process and take an active role in securing the organization.

Historical data suggests that attacks on nonprofit sites can be motivated by pure malice and not money. In 2008, the Epilepsy Foundation of America experienced a hack that left clients with migraines and near-seizure reactions after hackers bombarded the foundation's website with links to pages with rapidly flashing images. Flashing images can cause seizures for some with photosensitive epilepsy. According to Digital Journal, "the hackers found a security hole in the foundation's publishing software that allowed them to quickly make multiple posts and overwhelmed the site's support forums."

If the issue feels like a personal one for me, it certainly is. On a warm Saturday in August 2017 while picking up cupcakes for my granddaughter's first birthday, I paused in the parking lot to find a link on the Brain Injury Alliance of Arizona's website for a client. I typed in the website into the search engine on my phone, expecting the familiar to appear only to find the entire site completely gone. Immediately all the worst-case scenarios whirled through my mind — hacking, ransomware, something even worse.

It was a very long 20 minutes later that I learned our former technology company had initiated a server swap that did not go as planned with our primary host and all would be well within the hour. It was a lesson learned and a warning for me as I started to move malware scanners, firewalls and overall cybersecurity to the absolute top of my priority list. Nonprofits of all sizes would do well to head the warnings raised and blueprints for success laid out by the Business Journal article.

As our Valley professionals will tell you, in cybersecurity it's not if you get attacked — it's when.

Carrie Collins-Fadell *is the executive director of the Brain Injury Alliance of Arizona and a board member for the nonprofits* ***Because I Said I Would*** *and the* ***United States Brain Injury Alliance.***