# Outside Vendors: Protecting Your Data

***by Kara M. Curtis, CPA, Audit Manager***

Posted on August 4, 2021

We all know that technology is adapting and improving every day. Over the past decade, data has become much more accessible and cloud-based. While this provides many positive opportunities for users of the data, the threat of cybersecurity breaches has also increased. With so many organizations adding remote capabilities over the past year, these risks are even more exposed.

So why is this important to you? Unless your organization develops all of its own hardware and software, there is a good chance that a third party vendor is involved. Several studies performed over the past year have reported that the majority of data breaches were caused by giving too much access to a third party vendor with improper security measures in place.

Most organizations already have strong controls in place over their IT systems. Employees are typically required to sign agreements stating they understand and will follow the IT policies and procedures. You might assume that the vendors you are working with are reputable and would never inappropriately use your data, but what if that vendor gets hacked? Your organization's security controls may not be able to protect that vendor and your data could be at risk! So, how can you make sure that any third parties who access or host your data also have strong controls in place?

**Step 1: Identify third party vendors**

The first step is to identify who has access to your data or is hosting your data. These third party vendors can include (but are not limited to): financial reporting software vendors, web hosting services, cloud-based software applications, contractors, payroll processors, equipment maintenance vendors, external consultants, and even your auditors!

**Step 2: Determine access levels**

The next step is to identify their level of access. Third party vendors should only have access to the areas or modules needed for their assigned tasks. In many cases, read-only access is sufficient, but you can assess what areas are needed for full access. Organizations should also restrict vendor access in sensitive data areas such as personally identifiable information for employees, donors, customers, or students.

**Step 3: Discuss vendor controls AND document!**

Next, your organization should have a comprehensive discussion with these third party vendors to confirm they have the proper security controls in place to guarantee your data is protected at all times. This discussion should then be formalized into a written contract or data sharing agreement.

For Arizona school districts, this step is even more important because the *Uniform System of Financial Records for Arizona School Districts* (USFR) requires all school districts to ensure that proper data-sharing agreements or vendor contracts are in place before granting access or sharing data with third party vendors. The agreements/contracts should include a summary of the services provided, the specific security and processing integrity controls in place, the vendor's responsibilities, the district's responsibilities, and any backup procedures (if applicable). As a general rule, you want to make sure the vendor meets the security requirements of your organization (i.e. firewalls, up-to-date anti-virus, anti-spyware, anti-malware software, system patches, encryption measures, etc).

Most third party vendors will develop their own data-sharing agreements or vendor contracts that outline their security policies and procedures. If this is the case, your organization should request a copy of this document and maintain it for your records. If the vendor currently does not have an agreement like this in place, you could either: (1) request these security measures are included in their standard vendor contract before agreeing to the services or (2) develop your own internal agreement which includes the minimum vendor security controls required and have the vendor sign this agreement before services are provided.

**Step 4: Monitor**

In addition to having an agreement/contract in place, the district or organization should perform its own due diligence to check if vendors are properly following their policies and procedures. Districts and organizations should make sure to consistently review any data that was accessed or processed by vendors or third parties to make sure it was used appropriately and not mistakenly edited. This can be achieved by running electronic audit trail or change log reports on a frequent basis.

As technology continues to advance, your approach will change, but you always want to make sure you and your vendors are one step ahead!