

## School Districts to Undergo Cybersecurity Audit

**Articles** October 12, 2015

Missouri Auditor Nicole Galloway recently announced plans to conduct cybersecurity audits of five school districts. Coinciding with National Cybersecurity Awareness Month, the audits are intended to reveal how school districts protect the personal information of its students. Considering the amount of information school districts are entrusted with storing, it is surprising these types of audits have not been conducted sooner or on a wider scale.

School districts store a tremendous amount of personal information including educational records, health records, and financial information. Further, school districts do not just store the personal information of its students. The personal information of teachers and other employees is also at risk.

School districts must take steps to ensure this personal information is properly protected. Audits, as suggested by the Missouri cases, can be a good way to assess the security measures a school district has in place as well as identifying potential weaknesses.

For example, school districts rely on a number of vendors to provide the services needed to run its day to day operations. These vendors may include those third party entities that provide outsourced IT services, software platforms, and distance learning tools. Not properly vetting vendors is one common area of weakness in a school district's data security plan.

It is critical that school districts conduct sufficient due diligence of its vendors before purchasing their services. This due diligence must include an assessment the security measures the vendor has in place as well as its privacy policy. In addition, the school district must carefully review and negotiate its contracts with these vendors to ensure there sufficient security obligations are imposed with respect to any personal information they may store, transmit, access, or otherwise use in performing its obligations. These contracts must also provide for appropriate indemnification of the school district in the event a breach occurs.

Properly vetting vendors is just one way school districts can proactively reduce their risk of a data breach. Other best practices include maintaining a breach notification policy and providing periodic training on security issues for employees.

If you have questions regarding your school district's security risks, or if you would like to arrange for a security audit, please contact Kristin Biedinger at (412)594-3916 or [kbiedinger@tuckerlaw.com](mailto:kbiedinger@tuckerlaw.com).