Strike Graph

Is your edtech meeting security standards?

The current global pandemic has thrust the education industry into 100% online learning. Institutions and educators are desperately adopting edtech products to deliver learning to students.

Underneath all the talk about Zoom classes and online plans for September, is the critical need to keep institutional data private. This is very difficult when institutions are moving online almost instantly. Statistically, over 70% of breaches happen through a third-party. These breaches can be incredibly damaging. In July 2019 Pearson Education experienced a data breach affecting its AIMSWeb 1.0 platform. Roughly 13,000 school and university accounts were affected by this breach including millions of student records.

In times of great need like the current global crisis we have to look for ways to create rapid change but maintain some standard of trust. Thankfully there is a widely adopted standard that you can use to ensure the edtech vendors you are rapidly plugging into your technology infrastructure can protect students' private data.

That standard is called SOC 2 and it's become the audit standard across industries ranging from banking to high-tech.

In 2017 the American Institute of Certified Public Accountants (AICPA) published the Trust Services Criteria. The Trust Services Criteria defines the requirements and method for a company to be assessed by an independent auditor on cyber security practices. Like any good high-stakes assessment the auditor will produce a report of a vendor's ability to meet the standard that you can trust. A successful assessment by the auditor is called a SOC 2 certification and it's meant to create trust between you and your vendors.

As the banking and high-tech industries have already learned anytime you're sharing data with another company you should require a SOC 2 certificate. In speaking with the CEO of Strike Graph Justin Beals, I learned "Most commercial companies today require a SOC 2 certificate before allowing a new vendor to receive a contract. Microsoft, Bank of America, and Delta Airlines are all requiring vendors pass a SOC 2 audit annually. This is changing for education. We know that the State of North Carolina, DOE has started requiring a SOC 2 certificate of their vendors. This is a great sign as the educational industry moves beyond the self-reported FERPA to an independently audited standard."

There is an effective way for institutions to quickly trust new digital partners. A SOC 2 certification proves that your edtech has passed an independent assessment of security practices. Keep your institution safe by requesting a SOC 2 audit before you adopt. As educators share data more seamlessly, finding efficient ways to trust vendors is a critical practice.

If you're interested in learning more about SOC 2 email brian.bero@strikegraph.com.

ABOUT STRIKE GRAPH

Strike Graph is a compliance SAAS solution simplifying security certifications such as SOC 2 Type I/II or ISO 27001. These certifications dramatically improve revenue for B2B companies. Facilitated by the Strike Graph platform, key actors in the process including Risk Managers, CTO's, CISO's and Auditors can work collaboratively to achieve trust and move deals. For more information visit https://www.strikegraph.com.