Published on *The National Law Review* https://natlawreview.com

Is Your Student Information Adequately Protected?

Article By:

Burt Cohen

Daniel J. Kagan

Recently, educational institutions have become targets for hackers and the victims of significant data breach incidents. No institution is invincible from attack. Within the last two years, preeminent universities such as Harvard University and UC Berkeley were subject to attacks; however, hackers are not simply going after large post-secondary institutions, as hackers have targeted local school districts spanning from Massachusetts to California.

In a timely response, effective October 1, 2016, the Connecticut legislature enacted Public Act 16-189, "An Act Concerning Student Data Privacy." As the school year begins, now is the time for local and regional boards of education to take proper preparations for the effects of the law.

Generally speaking, the law imposes a variety of restrictions on how student information can be used. For example, the law requires specific contract provisions to be in agreements between a board of education and any software or information storage contractor. The law also imposes restrictions on website, online service and mobile app operators, specifically as to how such operators can use student information. In the event any contractor or operator experiences a breach of student information, such providers must notify the local or regional board of education without unreasonable delay, but in any event, no later than thirty (30) days, of such an incident. Violations of the law carry civil penalties.

In addition to complying with the law, a local or regional board of education can take preventative steps to help avert or mitigate the impact of a data breach incident. To help organize and consolidate all of the necessary action items, a local or regional board of education should execute and implement a written information security plan (WISP). A WISP would include many of the following preventative steps, including, but not limited to, having appropriate plans in place to not only adequately respond in the event of a security breach incident but to also train employees on the importance of information security. A WISP would also address the technical and physical safeguards that can help address data breach concerns. For example, technical safeguards would include information technology solutions such as increasing firewall protection, implementing spam/phishing filters and/or maintaining offline server back-ups; whereas physical safeguards could include adding locks on doors where student information is held. These safeguards work together to protect the confidential student information held by public educational institutions.

National Law Review, Volume VI, Number 231