Key points:

- **Strong response plan can help LEAs answer pertinent questions about student data breaches**
- **When breach occurs, act with urgency**
- **Require providers to give 'initial' notice well before allowable 30, 60 days**

Establish expedient response plans to student data breach, attorney says

As schools increasingly turn to software, web-based learning, mobile apps, cloud computing, and other electronic methods to improve student learning outcomes, experts agree that it exposes districts to a number of risks, the most concerning of which is compromised uses of students' personally identifiable information.

Connecticut is one of several states recently enacting laws that have made sweeping changes to the protection and use of student information.

The Act Concerning Student Privacy, Pub. Act 16-189, which went into effect Oct. 1, sets forth minimum privacy and contractual standards for all parties involved in the creation, use, or handling of student data.

For instance, upon notification of a breach of security by a contractor, a board of education must, within 48 hours, let students affected and their parents or guardians know when student information and records or student generated-content was involved in such a breach, according to the law.

The local or regional board of education must also post notice of the incident on its website.

While a board of education has just 48 hours to notify those involved of a breach, a third-party operator or consultant has 30 days in the case of student data, and up to 60 days in the case of student records and student-generated content, to notify the board of education when a breach has occurred.

That said, nothing prohibits a board of education to require in its agreements with a contractor or consultant who handles student data to notify the board of education within a shorter period of time, which is what attorneys at Shipman & Goodwin LLP recommended to local and regional boards of education.

Act with urgency

Bill Roberts, an associate with the firm, emphasized that the 30 and 60 day requirements constitute the "outer limits" for notification. In either case, an operator or consultant must give notice "without unreasonable delay," he said.

"We are concerned that 30 and 60 days may be too long to wait for a breach notification and that a board may want at least an initial notice in a shorter timeframe (e.g., an initial notice of the breach in 10 days and details about the breach 20 days later)," he said. "A board may desire an initial notice so that it can be involved in the breach investigation, ask questions of the operator, and provide information to students and parents in a prompter manner."

To prepare for breaches, he urged LEAs to have a breach response plan in place and to "never rely upon ... the goodwill of the operator or software company to give you what you need' in order to respond to parents and students when their information is compromised."

"We worry about parents complaining about hearing of a breach two months after it occurred," he said. "However, we are also aware that many breaches may be very challenging to investigate and that pertinent information may not be known to the operator for some time after the occurrence."

While 30 to 60 days is a common legal requirement, many entities -- including those in healthcare and finance -- push for shorter breach-reporting timeframes in order to mitigate any harm caused by the breach, he said.

If a breach were to occur, he said, school district leaders or their legal counsel should ask for the following information or some variation thereof:

- What happened?
- What type of information was involved in the breach?
- What date was data compromised?
- Which students were affected?
- How many students were affected?
- What did the operator do in response?

He said district leaders should act with urgency and be assertive in collecting this information, which is "best facilitated" by having a breach response in place beforehand.

"A good contract up front may reduce the need to be aggressive," he said. "If you don't require something in the contract, you should not expect an operator to voluntarily offer the information. Breaches may expose an entity to liability and, thus, an operator may be hesitant to share information absent a contractual requirement to do so."

Emily Ann Brown covers education technology and STEM education issues for LRP Publications.

October 26, 2016