New York: Reasonable InfoSec or Not Reasonable InfoSec? That Is The Question.

Monday, June 10, 2019

Last week, the New York State Senate, at the request of the state attorney general, passed the “Stop Hacks and Improve Electronic Data Security Act” (the “Shield” Act). The bill is currently working its way through the New York State Assembly and is expected to be signed by the governor once passed. The Shield Act creates affirmative data obligations, provides factors to determine whether information has been breached, increases civil penalties for failure to notify, and extends the statute of limitations on enforcement actions.

The Shield Act would create an affirmative data obligation on regulated entities to “implement and maintain reasonable safeguards” for the personal information being collected. One way to comply with these requirements is to implement and maintain an information security program.

The Shield Act provides the basis for a compliant information security program. Entities would be deemed to have reasonable safeguards that fulfill their affirmative obligation if it implements certain administrative technical and physical measures. More specifically, businesses can designate employees to coordinate the information security program, identify and address foreseeable risks, provide employee training, and require their vendors to comply with these standards.

To comply with the Shield Act, entities will also be required to maintain reasonable technical safeguards. Technical safeguards may include assessing risk in all computer networks, software and systems, and performing ongoing testing of the various data storage platforms. Entities will be required to have reasonable data disposal practices as well.

Despite New York’s current data breach notification laws, the New York legislature is using the Shield Act to supplement obligations for companies that expose data of New York citizens. They have provided new definitions and notification requirements. A breach is defined as an “unauthorized access to or of, or access to or acquisition without valid authorization” of data. In determining whether their data has been accessed without authorization, entities may consider (i) physical possession or control by an unauthorized person, (ii) indication that the information has been downloaded or duplicated, and (iii) the opening of fraudulent accounts or other evidence of identity theft.

This new legislation perpetuates the recent trend of jacking up fines and penalties on businesses that lose or expose consumer data. Entities that knowingly or recklessly violate Shield’s notification requirements would be subject to a civil penalty of at least $5,000 and up to $250,000. The Shield Act also gives the attorney general more time to bring claims against an entity by extending the statute of limitations from one year to three years after the earlier of (i) the date in which the attorney general became aware of the incident or (ii) the business sent notice to the attorney general.

Entities that own or license computerized data of New Yorkers should consider the Shield Act’s provisions when creating or updating their administrative and technical security procedures. Compliance with the Shield Act will
require diligence in contract drafting, human resources practices, and technical risk assessments.

Source URL: https://www.natlawreview.com/article/new-york-reasonable-infosec-or-not-reasonable-infosec-question