CEP Magazine - October 2021
Cybersecurity programs can shield organizations—compliance officers can lead them

By Yvette Gabrielian, JD, and Alan Brill, MBA

Yvette Gabrielian (yvette.gabrielian@kroll.com) is Senior Director in the Cyber Risk practice with Kroll's Los Angeles office. **Alan Brill** (abrill@kroll.com) is Senior Managing Director with Kroll's Cyber Risk practice in Secaucus, New Jersey, USA.

Connecticut was the third state, after Ohio and Utah, to codify what could be called an "incentive-based approach" for businesses to implement and maintain a cybersecurity program. The bill, which was signed into law in July 2021, has an effective date of October 1, 2021.[1] The law aims to reward companies by shielding them from punitive damages when they have created and maintained a written cybersecurity program with a proscribed set of objectives, scope, and components that correspond to one of the cybersecurity frameworks listed in the law.

At first glance, the law may seem to be a kind of "get out of jail free" card, but it decidedly is not. To qualify for protection under the law, a company must have a written cybersecurity program that is in line with one of a number of defined standards and/or laws. More importantly, the program must comply with administrative, technical, and physical safeguards that are properly implemented and maintained. That is, a company must be able to demonstrate that it was actually and consistently doing what its written cybersecurity program claimed it was doing.

Whether you focus on Connecticut's new law or similar laws in various stages of legislative review throughout the United States, having an effective compliance program associated with cybersecurity policies and procedures becomes central to a company's response to data breach incidents, and does so in several ways.