COSMOS
Navigate the Compliance Universe

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.

Before and after a breach

The need for a cybersecurity compliance program can be identified when looking at two common expectations found in US state cybersecurity laws.

First, there's a focus on an organization's cybersecurity compliance program as it operated *prior* to a breach. A company would be hard-pressed to claim that its cybersecurity program was effective without evidence that it was being monitored so that the degree of compliance—and noncompliance—with the program elements was a key design element of the program and served to provide ongoing assurance that the program was real, rather than aspirational.

Second, when a breach occurs, there is a need to be certain that any actions taken are clearly understood and documented. Whatever a company does, if its response causes the destruction or modification of critical data that could indicate what happened, who was involved (internally and externally), and what was done in response, it will almost certainly be a problem in future litigation. Issues like the "chain of custody" over digital evidence might sound like something that TV detectives talk about, but please understand that issues like that are very real and come up in civil litigation as much as in criminal cases.

Compliance professionals, we believe, are uniquely qualified to support both of these requirements. They already possess the skill set to conduct successful reviews and provide lists of opportunities for continuous improvement and maturing of the cybersecurity program. Their reviews can help establish the affirmative defense under Connecticut's law against claims that the breach was due to "failure to implement reasonable cybersecurity controls." Therefore, we advise—and this new set of legislation expects—that periodic compliance reviews be an integral part of a functional cybersecurity program. Failure to do so will bring the effectiveness of a company's cybersecurity into question and will likely result in losing the company's shield against punitive damages.

There must be recognition from leadership that compliance is a part of the cybersecurity equation from its initiation and that appropriate resources needed for a meaningful review must be defined and provisioned. It is no longer a nice-to-have or proactive add-on that companies can choose to leave out. These new laws are making it clear that to take advantage of the shield, companies must invest the appropriate resources not only in the cybersecurity program, but in compliance activities. This informs management whether the program is working and to identify necessary changes to assure compliance.

Compliance and broader cybersecurity efforts

The suggestion that compliance should contribute more broadly to cybersecurity represents both a challenge and an opportunity for compliance professionals. They can be the proactive team to help the information security department in its efforts to improve and mature the company's cybersecurity program. Further, when an incident occurs, compliance professionals can play a key role in the response.

As part of any effective cybersecurity program, there must be a well-thought-out incident response plan. Your role as a compliance professional must be defined in the plan. It should not be an afterthought. You should assume responsibility to track resources used and the actions taken. You can also help to secure evidence and provide assurance that it is protected. You can work with external resources in the fields of forensics and investigation to understand what has already been done. Long term, you can help identify and implement improvements in the cybersecurity program to ensure a similar incident does not occur again.

A call to action

Cybersecurity laws like in Connecticut are calls to action for compliance professionals. Without your skills and abilities, how can an organization demonstrate that its program—no matter how well it tracks the program requirements set by the chosen standard—is working? How will it demonstrate that its incident response program was tested and performed effectively? Good intentions are not enough, so expect to show that the incident response program outlined all steps in advance of an issue.

An organization ignores those questions at its own peril. Compliance has a key role, and it should be proactive in addressing it and carrying out the necessary requirements. Without forethought, a well-intentioned cybersecurity program will become noncompliant with the requirements of the law.

About the authors

Yvette Gabrielian is an attorney specialized in cybersecurity and data privacy with more than 14 years of experience in compliance and corporate governance.

Alan Brill is a fellow of the Kroll Institute. He is also an adjunct professor at the Texas A&M University School of Law.

Takeaways

- Stay ahead of the changes that can be expected as cybersecurity laws evolve and come into fruition.
- Be proactive in identifying the expanded role of the compliance department associated with the requirements of these "safe harbor" laws or regulations.
- Align your department's skill sets and abilities to fit the new need. Identify and acquire the resources required to assure compliance with these new laws.
- Educate management on the need to implement compliance features into the cybersecurity program to protect the organization under the new laws.
- Work with IT, legal, and other departments to determine how compliance can be integrated into the cybersecurity program, and demonstrate that compliance resources are available.

1 Substitute H. B. 6607, Pub. Act No. 21-119, An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses (Conn. 2021), https://bit.ly/3jhHm5w.