CARLTON FIELDS

Is Your Organization Ready for the CCPA? The Importance of an Incident Response Guide

July 03, 2019

An incident response guide is the organization's playbook for how to investigate, respond to, and remediate a data security incident or breach. The best guides are short, easy to follow, and clearly lay out roles and responsibilities — and contact information — for the organization's incident response team. The team should be familiar with the guide from conducting tabletop exercises and revising the document periodically.

The benefits of a functional and well-tested guide are widely known. As an initial matter, the process of drafting a guide prompts an organization to evaluate its cybersecurity posture, identify risks, and marshal resources to be ready for an incident. When there is an incident, the guide should help the organization identify and respond in a more timely and disciplined manner, which can dramatically cut down on response costs. In fact, the Ponemon Institute's annual survey of data breach costs routinely notes that response costs are lower when data breaches are identified and contained as quickly as possible.

The CCPA's looming effective date underscores the need for an incident response guide. Among other things, the CCPA confers a private right of action — with statutory damages ranging from $100 to $750 per consumer per incident — for breaches involving personal information that result from an organization's failure to "maintain reasonable security procedures and practices." This private right of action, which explicitly permits class actions, means that organizations subject to the CCPA must assess their cybersecurity posture as part of their preparations. That assessment includes ensuring that an incident response guide is in place. The guide will help the organization detect and respond to a potential incident, possibly preventing that incident from amounting to a breach that could give rise to a claim. And if there is litigation, the presence of an incident response guide will be among the features that defense counsel will tout in defending the organization's "reasonable security procedures and practices."

The CCPA heralds a new era for cybersecurity and privacy in the United States, and getting ready for the law is no small task. Organizations would be well-served to update and test their incident response guides now so that they can focus on other, more labor-intensive aspects of their CCPA preparations.

Related Practices

Cybersecurity and Privacy
Cyber Insurance Coverage Disputes