CCPA: Implementing the Right Cybersecurity Plan Is Now a Legal Issue

11.19.2019

Addressing cybersecurity risks invariably involves very technical matters. As a result, in many companies the IT department has been responsible for developing and implementing cybersecurity plans and procedures. However, once the California Consumer Privacy Act (CCPA) takes effect on January 1, 2020, legal departments will need to play a much larger role, as businesses that suffer a data breach may become subject to a private right of action that provides statutory damages of between $100 and $750 "per consumer per incident or actual damages, whichever is greater." Cal. Civ. Code § 1798.150(a)(1). This private right of action only applies to a certain subset of personal information protected under the CCPA, specifically, an individual's name along with his or her:

- social security, driver's license, or California identification card number;
- account, credit card, or debit card number, in combination with a code or password that would permit access to a financial account; or
- medical or health insurance information. Cal. Civ. Code § 1798.81.5(d)(1)(A).

There are several measures that a company can take to mitigate this risk. One is to encrypt or redact the personal information, as the statutory damages only apply to "nonencrypted or nonredacted personal information." Cal. Civ. Code § 1798.150(a)(1). Another is to implement "reasonable security procedures and practices appropriate to the nature of the information." Cal. Civ. Code § 1798.150(a)(1). Unfortunately, neither the CCPA nor the California Attorney General's recently proposed regulations provide greater clarity as to what is considered reasonable or appropriate.

However, there are several resources that should provide adequate protection if followed in developing a cybersecurity plan. For example, a recent Ohio law provides a safe harbor from the state's data breach provisions for companies that have implemented cybersecurity plans that reasonably conform with any of the following recognized frameworks:

- NIST Special Publication 800-171;
- NIST Special Publications 800-53 and 800-53a;
- National Institute of Standards and Technology's ("NIST") Cybersecurity Framework;
- The Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework;
- The International Organization for Standardization/International Electrotechnical Commission 27000 Family—Information Security Management Systems;
- The Center for Internet Security Critical Security Controls for Effective Cyber Defense.

Presumably, a California court would agree. In addition, NIST, a non-regulatory agency of the United States Department of Commerce, recently published a preliminary draft of the “NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management.” The final publication should also provide supportable guidance on developing and implementing appropriate plans and procedures.

Regardless of what approach is taken in developing and implementing a cybersecurity plan, it is now important for companies that may be subject to the CCPA to include legal counsel in the decision-making process as to whether the plan is adequate from a legal standpoint. Even if a company determines it is not subject to the CCPA, having legal input on cybersecurity protection will increasingly become important given the growing convergence of data protection and cybersecurity.

Related People

- Kevin D. Pomfret – 703.760.5204 – kpomfret@williamsmullen.com