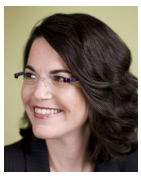
California Attorney General Announces a Standard for Reasonable Data Security



by Batya F. Forsyth

On February 16, 2016, the California Attorney General issued the "California Data Breach Report: February 2016" (the Report) analyzing data breaches reported to it from 2012 to 2015. The information about reported breaches provides useful insights into where businesses can best defend against data breaches. Notably, the Report also announced a standard of data security that will be relevant to State data breach enforcement actions.

California law requires businesses to “implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.” Cal. Civ. Code § 1798.81.5. Security companies, non-profit groups, and government organizations have provided guidance on good security practices, but no California statute, regulation, or attorney general opinion defines “reasonable security practices and procedures.” The Federal Trade Commission has also been at work defining reasonable data standards, with the Third Circuit recently holding that FTC publications as well as published settlement actions are sufficient to put businesses on notice of what are reasonable data security practices. *Federal Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

The Report recommends implementing a set of standards called the Critical Security Controls (the Controls). The Center for Internet Security, a non-profit organization, developed the Controls. The Center promotes the Controls as actions every enterprise should take to secure its data and systems. There are 20 controls listed as well as sub-controls tailorable to different types of business needs ranging from technological (e.g., keeping systems and software up-to-date) to administrative (e.g., ensuring employees may only access information they need). While the Controls allow each business to choose a proportionate way to meet each requirement, the Report makes clear that "failure to implement all the controls that apply to an organization's environment constitutes a lack of reasonable security."

We can infer from the Report—although it does not state directly—that the Attorney General will look to the Controls as enforcement guidelines in the absence of any particular statute, case, or regulation providing a definitive interpretation. On

another level, the interest in providing enforcement guidelines also may signal that the Attorney General intends to step up enforcement against companies that fail to implement what are deemed reasonable security procedures and practices.

Strong data security programs incorporate technological tools, written policies, employee training and oversight across the entire enterprise directed toward detecting, preventing, and mitigating data breaches. The Controls should be consulted in conjunction with other legal requirements in order to bolster the defensibility of those programs.

Hanson Bridgett's Privacy, Data Security and Information Governance Practice Group is available to provide counsel and assistance in addressing changing regulatory standards and new legal developments.

For more information, please contact:

Batya F. Forsyth, Partner
415-995-5827
bforsyth@hansonbridgett.com