Cooley

Reasonable Security Defined: California Attorney General's 2016 Data Breach Report

March 2, 2016

On February 25, 2016, the Office of the California Attorney General released its 2016 California Data Breach Report, which contains a compilation and analysis of the information provided to the Attorney General pursuant to data breach notification requirements. The data paint a picture of a data security problem that is far from solved and that is concerning for companies and consumers alike.

Companies may be equally interested in recommendations that the Attorney General made in an attempt to help companies reduce the risk of data breaches and mitigate the harms that result from such breaches. While not binding, the recommendations provide a window into how the Attorney General's office may exercise its investigatory and enforcement powers against companies suffering data breaches and, critically, set out the Attorney General's view of what constitutes a minimum for "reasonable security" to satisfy the "standard of care for personal information."

"Data breaches are growing in scope, affecting more organizations and more people."

The Report's headline-grabbing revelation is that nearly three in five Californians (approximately 24 million records) were affected by a data breach in 2015 – nearly six times the 4.3 million Californians affected the year before. In 2015, however, the total number of data breaches itself remained relatively flat. This seeming disparity in cause and effect results from a handful of large (and well-publicized) breaches like those suffered by Anthem (affecting 10.4 million Californians) and UCLA Health (affecting 4.5 million Californians). The Report also breaks down data breach trends over the four years that the reporting requirement has been in effect:

- In total, 657 data breaches have affected over 49 million records of Californians in the last four years.
- While the number of breaches has risen only slightly during this period, the number of Californians affected has fluctuated dramatically as a result of the handful of extremely large data breaches:
  - 2012 – 2.6 million
  - 2013 – 8.5 million (the year that included the Target and LivingSocial data breaches)
  - 2014 – 4.3 million
  - 2015 – 24 million, a record high
- Retail companies appear to be particularly vulnerable, accounting for 25% of all breaches and a disproportionate 42% share of all records breached between 2012 and 2015.
- Finance and healthcare industries were the second and third most likely to suffer a data breach, accounting for 18% and 16% of breaches, respectively.
- The primary and ever-increasing threat to businesses comes from malware and hacking breaches.
  - These breaches account for 54% of all breaches during the four-year period
  - The number of breaches resulting from malware and hacking has nearly doubled since 2012.
- Breaches resulting from physical theft and loss, on the other hand, have decreased, a fact the Report attributes to the "more widespread and effective use of encryption."

The Attorney General's pronouncement on the minimum requirements for "reasonable security."

As a result of its analysis of four years' worth of data, the Attorney General has made four recommendations for

companies handling personal information:

1. Implement the 20 controls in the Center for Internet Security's ("CIS") Critical Security Controls ("CSC" or "Controls") "that apply to [the] organization's environment";
2. Expand the use of multi-factor authentication to protect consumer-facing online accounts that contain sensitive personal information, including online shopping accounts, health care patient portals, and web-based email accounts;
3. Use strong encryption to protect personal information on laptops and other portable devices, and consider using the same encryption on desktop computers; and
4. Encourage individuals affected by a data breach to place a fraud alert on their credit files.

The first of these recommendations will likely prove to be the most significant. Indeed, the "recommendation" that companies implement CIS's Controls is framed as a directive, with the Attorney General taking the position that the 20 Controls "define a minimum level of information security that all organizations that collect or maintain personal information should meet," and that "failure to implement all the [applicable] Controls … ***constitutes a lack of reasonable security***" (emphasis added).

For those who have never heard of the CIS Controls, the Report describes them as "a consensus list of the best defensive controls to detect, prevent, respond to, and mitigate damage from cyber attacks," "updated periodically to keep up with technological advances and changing threats." Appendices A and B to the Report set out all 20 Controls. The Controls generally represent a three-pronged approach to data security: implementation of security technology, control of information, and training and preparedness. So, for example, CSC 8 calls for the implementation of "malware defenses," while CSC 14 calls for "controlled access [to information] based on the need to know," and CSC 17 requires "security skills assessment and appropriate training to fill gaps." Importantly, the Report calls the Controls a "***starting point*** of a comprehensive program to provide reasonable security" (emphasis added).

What does this mean for companies? While the recommendations are not binding, the Report suggests that the Attorney General's office could exercise its investigatory and enforcement powers if companies experience data breaches and have not implemented the applicable Controls or followed the Report's other recommendations. These recommendations may also serve as a reference or template for other regulators. The Report acknowledges, however, that companies should assess which Controls make sense for their business. At a minimum, given the position taken by the Attorney General in the Report, the Controls should be a consideration in companies' data security planning.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Matthew D. Brown San Francisco	brownmd@cooley.com +1 415 693 2188
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.