WilmerHale

Recommendations from California's Latest Data Breach Report

FEBRUARY 22, 2016

As the state that began the data breach notification trend, California continues to play an important role in setting data security trends. In a data breach report released this week, the California Attorney General's Office noted an increase in both the number of data breaches and the size of those breaches since a 2012 legal requirement mandated businesses report breaches to the Attorney General. Last year alone, 178 breaches ensured that nearly three in five Californians were the victims of a data breach.

Thanks to a considerable amount of number crunching on the part of the Attorney General's Office, there are some clear trends that appear in the report. Malware and hacking present the greatest security threat ahead of physical breaches and employee error. And malware and hacking is a problem that is growing. Across industry sectors, retailers are the primary source of data breaches, and as expected, most of their breaches are caused by malware and hacking that target credit card information. The transition to chip-enabled payment cards could diminish the attractiveness of stealing payment card data as criminals instead turn their focus to obtaining Social Security numbers, which already rank as the most likely bit of information to be breached.

Four recommendations based on "lessons learned" from reviewing four years of data breaches make up the crux of the report. In general, the recommendations provide a minimum standard of care for personal information and suggest companies embrace three specific practices. The report also has some sharp commentary on the proliferation of state breach laws since 2003 and potential federal action in response.

1. **Adopt the Center for Internet Security's Critical Security Controls:** The report calls on businesses to adopt reasonable security that "starts with basic privacy practices." Existing guidance from the Federal Trade Commission is highlighted, as are influential security standards such as NIST's Framework for Improving Critical Infrastructure Cybersecurity and ISO/IEC 27002:2013.

The Center for Internet Security's *Critical Security Controls for Effective Cyber Defense* is specifically offered as a helpful starting point for "synthesizing all of this information and prioritizing the actions to take." Importantly, the report notes that the failure to implement these controls "constitutes a lack of reasonable security."

According to the report, many of the breaches highlighted over the past four years could have been arguably prevented or detected had basic security controls been implemented. These controls encompass an organization's efforts to understand the hardware and software connected to its network; security configurations and user privileges; continual assessment, protection, and defense, including monitoring and testing; and employee training.

2. **Embrace Multi-Factor Authentication:** The report is clear on one thing: usernames and passwords are failing as a safe or truly effective means of authentication. Instead, according to the report, businesses—particularly consumer-facing entities—should move toward using multi-factor authentication methods to protect critical systems and data. The report highlights the special need to protect email accounts as they generally provide a digital gateway to any number of services or sensitive information, but it also stresses the need to embrace multi-factor authentication for online shopping accounts, health care websites, and patient portals.

3. **Encrypt, Encrypt, and Encrypt Some More:** As we engage in a national conversation about encryption policy, the California Attorney General notes that "[e]ncrypting data on portable devices could have prevented breaches that affected more than 2.7 million Californians." Businesses, with an emphasis on the health care sector, are called upon to implement strong encryption on laptops, portable devices, and even desktop computers. This applies to businesses large and small, as the report argues that "[a]ffordable solutions are widely available" and companies "owe it to their patients, customers, and employees to do [encryption] now."

4. **Encourage the Use of Fraud Alerts:** In place of cumbersome and costly credit freezes, fraud alerts are proposed as a "fast, free, and effective" method of combating new account fraud. Businesses are recommended to encourage victims to use fraud alerts whenever Social Security numbers or driver's license numbers are breached. While current data breach notifications frequently mention fraud alerts, the report laments that this information is "most often buried in the details" and encourages companies to make information about fraud alerts "more prominent in their notices."

Finally, the report takes aim at proposals to create a federal data breach notification law. It charges that most proposals under consideration by Congress "set the consumer protection bar very low." Further, these proposals would "infringe on state-based innovation" and eliminate "the highest-common-denominator approach" that effectively provides California-level protections in many jurisdictions.

Rather than a federal law, state-level policymakers should work together to "harmonize" any perceived "patchwork" of state breach laws. According to the report, any patchwork is primarily in three areas: (1) notification triggers, (2) timing for notification, and (3) what personal information is covered. Instead of navigating a patchwork, the Attorney General suggests that companies can avoid any problems by complying with the highest applicable standard. Moving forward, the report concludes by suggesting that state legislators and Attorneys General collaborate to highlight the similarities among state breach laws—and to reduce some of the differences.

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome.