Calif AG Reports On Breaches; Calls For More Encryption

from The Privacy Times

HARRIS REPORT: MAJORITY OF BREACHES INVOLVED SOCIAL SECURITY NUMBERS

California Attorney General Kamala Harris July 1st issued a report describing the data-breach notifications her office received from companies in 2012. The report provided recommendations based on those findings. A central recommendation is that companies encrypt sensitive personal information.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Last year, California enacted SB 24, amending the California breach law to require any organizations sending a security breach notification to more than 500 California residents as a result of a single breach also submit a copy of that notification to the Attorney General. Ten years ago, California became the first State in the country to pass a data-breach notification law (SB 1386, Cal. Civil Code Sections 1798.29 and 1798.82).

Harrisâ€™ office received reports of 131 data breaches affecting more than 500 Californians, involving 103 different entities regarding incidents reported in 2012. Nine of those 103 entities reported more than one breach â€“ three of those were payment card issuers where the breach occurred either at a merchant or at a payment processor.

The average breach incident involved the information of 22,500 individuals, but the median breach size was 2,500 affected individuals. Five of the reported breaches involved more than 100,000 individuals. It is not clear whether these

statistics refer only to California residents.

The sectors reporting the most data breaches in 2012 included retail, finance, and insurance. The AG classified as retail breaches of payment card account numbers that occurred in merchantsâ€™ systems, even where the payment card issuers notified consumers.

More than half of the breaches involved Social Security numbers (SSNs). Surprisingly, in 29 percent of the breaches involving Social Security numbers or driverâ€™s license numbers, no credit monitoring or other mitigation product was offered to the victims. (Credit monitoring or a similar â€œidentity theft protectionâ€• product was offered in 50 percent of the total breaches.)

Harris used "taxonomy" to classify breaches into three categories: physical, logical, and procedural. The breaches were then further broken down into more specific categories (respectively, document, media, and hardware; insiders and outsiders; and processing and disposal).

More than half of the breaches were the result of logical failures, i.e., intentional access to data by outsiders or unauthorized insiders. Fifty-five percent of the breaches involved intentional intrusions. Although breaches resulting from physical failures constituted 27 percent of the total breaches, they accounted for 58 percent of the victims. Breaches were reported to the AG an average of 12 days from notification of the affected individuals. Twenty-five percent were reported before or on the same day and 63 percent within 10 days, the AG report stated. (http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-releases-report-data-breaches-25-million)
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow ACCESS