Blog for MPA Networks

https://www.mpa.com/blog.aspx?p=data-breaches-california-information-and-prevention

Data Breaches: Dark Times in the Golden State?

Posted July 1, 2016

Being the cyber-security geeks we are, we took great interest in combing through this year's California Data Breach Report, released by the Attorney General's office this past February. The report tabulates data collected from breach incidents which expose confidential information of 500 or more individuals, reported to the Attorney General as required by California law since 2012.

Over these past four years, there has been a total of 657 reported incidents, affecting over 49 million Californians—from Social Security and driver's license numbers to financial accounts to health records, logins, and passwords.

By the Numbers: Not Much News to Us

The breakdown of California data breaches came as little surprise to us:

- **Malware and hacking** accounted for over half of all breaches (54%), while responsible for a whopping 90% of all stolen personal records.

- While **physical breaches**—lost or stolen unencrypted data on computers and mobile devices—came in a distant second (22%), they were the most reported by healthcare providers and small businesses.

- Other breaches were attributed to **human error** (17%) or **intentional misuse** or unauthorized access by company insiders (7%).

After 178 reported major breaches in 2015 alone, the report estimates almost *three in five* Californians were victims of loss or theft of data.

Plug the Leaks, Block the Hackers

The second half of the report offers multiple recommendations for preventing data breaches in the future. Specifically discussed is the expanded use of **multi-factor authentication** (as we've already recommended) in place of simple, easy-to-guess user passwords such as “qwerty” or “12345” (as we've likewise lamented in a previous post). **Stronger encryption standards** are needed to protect confidential data, particularly within the healthcare sector.

However, the Attorney General's primary recommendation is that all business and government organizations adopt their own risk management strategy based around the Critical Security Controls for Effective Cyber Defense, a comprehensive 20-point plan developed by the Center for Internet Security.

While a mishmash of federal and state-to-state regulations offer varying effectiveness against data breaches, the California report cites voluntary compliance with the CIS Controls as "a minimum level of information security that all organizations that collect or maintain personal information should meet," while falling short of the full 20 standards constitutes "a lack of reasonable security."

We agree the CIS Controls represent a solid roadmap, effectively "covering all the bases" when it comes to data protection. **When you discuss security with a potential MSP partner, mention the CIS Controls as a baseline.** If they downplay such a structured approach, you're probably talking with the wrong vendor. How well is your company meeting California's data security guidelines? For a few tips on getting better, ask us today.