Data Breach Risks for Law Firms

July 5, 2017

RELATED PRACTICES Retail, Privacy and Cybersecurity, Litigation

The term “data breach” usually brings to mind the much-publicized capture of vast quantities of consumer information from retail vendors (*e.g.,* Target, Windham), on-line service providers (*e.g.*, Yahoo!), or social media sites (*e.g.*, Ashley Madison). Hackers’ motives are presumably as diverse as the hackers themselves, but clearly include obtaining marketable information, such as credit card numbers and intellectual property, or embarrassing consumers, as in the Ashley Madison breach. Recent events also show that motives now possibly include political agendas with media reports that foreign hackers may even attempt to influence U.S. elections. Of course all this activity is criminal. “Guccifer,” the Romanian hacker involved in the disclosure of Hillary Clinton’s private email server when she served as Secretary of State, was extradited from his home country and recently sentenced to 52 month of prison after a plea bargain.

As this article shows, law firms are also prime data breach targets because they too hold vast quantities of commercially valuable information in their stores. For example, law firm servers harbor patent applications, merger and acquisition information, and litigation work-product, all of which might make hackers and their sponsors very rich. This article first explores why hackers target law firms and what are counsel’s obligations in light of this threat. The article then explores the consequences of a data breach in terms of the potential civil litigation and government enforcement actions. Finally, the article lists some of the tangible steps that a firm can take to protect itself from breaches and the consequences thereof.

Co-authored and co-presented for the State Bar of Texas Annual Meeting. To read the full article click on the PDF linked below.

Data-Breach-Risks-for-Law-Firms.PDF

© 2026 Haynes and Boone, LLP