THE
NATIONAL LAW REVIEW

Legal Lessons of Data Breaches

Tuesday, September 1, 2015

Article By James J. WardBilzin Sumberg
Philip R. SteinHomebuilder Blog

Communications, Media & Internet
All Federal

Every business would love to find a fortune teller to give it insight into what trends to follow, which risks to take, and when "exposure" will convert to liability. Some clients might say that, unfortunately, their lawyers are more Magic-8 ball than crystal ball – attorneys' responses to future-looking questions often sound a lot like "reply hazy, ask again later." To an extent, that is unavoidable. Lawyers, for good reason, tend to be particularly cautious with respect to advising clients as to what the future might hold. Giving a concrete answer based on today's best guess may lead to a lawsuit when tomorrow's reality conflicts with that guesswork.

But advice is only useful when it's timely, and there is a compelling argument that the future is now when it comes to the need for absolute vigilance about data security. Attorneys cannot simply advise clients about past precedents pertinent to this subject matter area; they must embrace the difficult task of trying to "see around corners." They must attempt to help clients anticipate not merely what data security protocols will be necessary to stay ahead of determined hackers, but also what future data security regulations might look like.

The last two years offer no shortage of cautionary tales about companies that did not take the time to develop necessary data security and privacy protocols. Some of them were well publicized – but most were not. Nearly everyone saw the media frenzy around Target's massive data breach, but did you know about Anthem? Dairy Queen? Neiman Marcus? P.F. Chang's? Or about the Ashley Madison prequel, last July's Adult Friend Finder hack?

The point is that the majority of data breaches are not national or even local news. They are well catalogued here, in a depressingly long list that includes some shocking allegations about professional sports teams and evidence of dilatory government security standards. Hundreds of millions of private records are accessed unlawfully every year, often without anyone ever knowing.

What does this mean? It means that there is a need to recognize the scope of the data security problems we face in this country. This is not a situation for which slapping a patch here, or changing passwords there, will suffice. We need a fundamental change of thinking when it comes to data security, and attorneys can help bring about the changes needed.

As we move closer to the Internet of Things, data's centrality in our lives, our businesses, and our communities will only deepen. That's no different for lawyers – and the problems will not only be about the client's data security. The practice of law already involves daily questions about how best to preserve client confidentiality, access and manage electronically stored information, and protect client data security. As attorneys become more aware of the need to protect their clients' sensitive information, they can, and should, advise clients about how best to protect their own data, and avoid the liability traps that others have failed to recognize.

Discerning where and how your business faces risk is a difficult task, but it should never be impeded by a refusal to learn. A thorough and honest appraisal of what you (and your lawyer, or your client) know about data security is a crucial first step in preventing a business with which you are involved from winding up in the Data Breach Hall of Shame. You don't need to be a fortune teller to see that shoring up your business's data security on a recurring basis will be an unmistakably important aspect of being #datasmart.

© 2019 Bilzin Sumberg Baena Price & Axelrod LLP

Source URL: https://www.natlawreview.com/article/legal-lessons-data-breaches