THE
NATIONAL LAW REVIEW

Less is More: The Role of Data Retention Policies in Cybersecurity Preparedness

Friday, October 26, 2018

We're all guilty of it. We keep things that we don't need, like that pair of stone-washed jeans from 1992 that you hope will come back into style or your beanie baby collection that you blindly believe might be worth something someday. While our inability to purge old stuff from our closets may cost us closet space, the repercussions for an organization that hoards data are far more significant. From a cybersecurity perspective, the more personal information a company maintains, the more information it has to lose. Consequently, the more information a company loses, the higher the financial and reputational costs.

Article By Daniel J. Kagan
Dena M. Castricone Murtha Cullina
Privacy and Cybersecurity Perspectives

Communications, Media & Internet
Global
Financial Institutions & Banking
New York
European Union

It's important to note that some data privacy laws require organizations to only keep data as long as necessary, such as the European Union's General Data Protection Regulation, the Children's On-line Privacy Protection Act and the New York Department of Financial Services Cybersecurity Requirements, to name a few. However, even if those privacy laws do not apply to your organization, there are also other practical considerations for proper information retention. These considerations include reducing paper and electronic storage costs and keeping litigation costs down during discovery because there will not be excess data to retrieve, search or turn over.

One thing has become clear over the past several years: breaches of electronic data are inevitable. Certainly, an organization should take all reasonable measures to prevent those breaches but it should also implement a mitigation strategy to ensure that, if there is a breach, there is as little damage as possible. That mitigation strategy includes incident response planning and training as well as ensuring that an organization only retains the data it needs to operate its business. This requires that an organization adopt data retention policy.

When creating a data retention policy, organizations need to assess whether it needs all of the information it collects and the applicable legal requirements for retaining such information. Clearly, if the law requires an organization to maintain records for a particular amount of time (such as medical records or information subject to a legal hold), then the organization must comply. If there is no legal requirement, then the organization will have to determine the business need for the information and the appropriate length of time to maintain it.

Finally, as with any policy, the organization must implement the policy and ensure that it is destroying data in accordance with that policy – no exceptions for fashion relics or potentially valuable collectibles.

Source URL: https://www.natlawreview.com/article/less-more-role-data-retention-policies-cybersecurity-preparedness