ACC DOCKET

INFORMED. INDISPENSABLE. IN-HOUSE.

Preparing for a New Era of Third-party Data Management

Law Department Management

Content sponsored by Exterro

As legal professionals at all levels — in-house corporate attorneys and outside counsel alike — assist their organizations and clients in complying with substantial, global changes to the way personal data is regulated, there is one area that is sometimes overlooked: third-party data ownership.

By some estimates, organizations are more at risk of an indirect data breach than a direct one. A Ponemon Institute study found that 61 percent of companies surveyed found that they had experienced a data breach due to lax third-party cybersecurity. What's worse: 66 percent of the companies that were breached didn't have an inventory of which vendors and other third parties had access to their data.

Susanna MacDonald, VP and chief legal officer at the Association of Corporate Counsel (ACC), didn't have this data handy when she was pursuing a third-party vendor risk solution — but she knew innately that third-party access to sensitive data was a growing concern.

“One of the things that I had to stress to my team was to look at third-parties in a very different, holistic way,” says MacDonald. “You have to think along multiple lines to determine whether you're sharing and storing data, and how much, with vendors that have access to sensitive areas of your organization.”

ACC today uses Exterro's Vendor Risk Service as a new way to manage all of the necessary information regarding ACC's third-party relationships. After reviewing all of her vendors using Exterro VRS, MacDonald is able to quickly and easily identify which vendors pose risks due to data privacy regulations or other compliance rules.

“Add in the importance of keeping all of your employees aware of the cyber diligence that needs to be done within an organization, because it's truly everybody's job to ensure the protection of the organization's data security,” says MacDonald.

For those organizations seeking a stronger grasp on their third-party relationships, MacDonald recommends determining answers to the following five questions:

- Who are our vendors?
- Which ones touch our data?
- What specific data do they touch?
- Which ones are relevant to regulations?
- How are they protecting our data?

And if vendors have security issues that concern your organization, press for change.

“Most of the vendors that we identified issues with were more than willing to put into place the resolutions that would help them be more compliant with the standards that we were looking for,” says MacDonald. “You have to maintain that vigilance.”

To learn more, visit Exterro.com.

Marty Provin

Vice President of Data Privacy

Exterro

Marty Provin is VP of data privacy at Exterro and has over 25 years of experience in information technology and governance. Provin advises in-house counsel, compliance, IT, and privacy professionals in the areas of information governance, data mapping, data minimization, and third-party diligence to comply with GDPR, CCPA, and expanding data privacy regulations. He is a Certified Information Privacy Professional (CIPP) and a frequent contributor and speaker in the legal and privacy communities.