Readjusting Cloud and Data Privacy Predictions

This year's sudden, unexpected need for cloud capabilities has helped to shift a very important learning to the forefront: Privacy and security are not corners you can cut. While the need to quickly migrate to the cloud is understandable, it is just as important to implement the necessary steps to reduce the risk of data exposure.

At the beginning of each year, experts from across industries share predictions, highlighting what they believe will be the biggest trends in the coming 12 months. It is fair to say that 2020 has thrown quite a curveball, creating business needs that none of us could have predicted. Take corporate America's rapid transition to a nearly exclusive remote work environment, which has forced many businesses to accelerate cloud migration plans to ensure productivity and business continuity.

While the need to quickly migrate to the cloud is understandable, it is just as important to implement the necessary steps to reduce the risk of data exposure — even if migration is delayed. With this in mind, forward-thinking organizations are taking specific steps to address immediate and long-term privacy and security needs. Such steps include taking a DataSecOps approach, supplementing security with privacy, and creating data-focused leadership roles.

(Link to the Full Article)

CPRA Could Bring Stricter Data Privacy Enforcement: Here's How To Prepare

California's passage of the California Privacy Rights Act (CPRA) on November 3 builds upon the California Consumer Privacy Act (CCPA). The EU's privacy regulation, GDPR, is the gold standard in terms of data privacy laws, and CPRA gets closer to that standard by reflecting society's increased desire for data privacy. Additionally, CPRA gives consumers even greater control over and access to personal data collected by companies than what CCPA did.

For covered entities, this may feel like a regulatory "one-two punch" because CCPA was just signed into law in January, with enforcement commencing in July. The good news for businesses is that CPRA will not go into effect until 2023, which gives businesses time to institute the necessary infrastructure to comply. While CPRA has many facets that must be examined, as explained by IAPP in May, I believe there are three areas of the new law that bring significant challenges as they relate to data protection:

• Creation of the California Privacy Protection Agency (CalPPA).

• Creation of the sensitive personal information category.

• Expanded consumer rights and data controller compliance.

(Link to the Full Article)

Data Protection Officer Responsibilities and Role Importance

Although there are numerous privacy laws and regulations that a data protection officer (DPO) can help organizations maneuver, the DPO role is most often associated with the formal requirements of articles 37 to 39 of the European Union's GDPR, explained Sal Aurigemma, associate professor of computer information systems at the University of Tulsa. The GDPR requires all companies that collect or process the personal data of EU residents to develop policies and procedures covering the collection, processing and management of personal data.

It's also important for companies to consider the DPO's role in facilitating collaboration across various stakeholders, including customers, businesses and regulators to gather, use and share information in a manner that is appropriate, legal and beneficial to all sides. Since the EU's adoption of GDPR, demand for DPOs has been steadily increasing across enterprises.

"Like the ombudsman, the DPO is the customer's advocate at a business to make the tradeoff between the utility of the data to the business and the trust contract with the customer to ensure that the data is utilized appropriately," said Ameesh Divatia, co-founder and CEO of Baffle, a cloud data protection company.

This will require astute diplomacy tactics to determine the correct tradeoffs. The risks of doing this poorly can include fines, loss of customer support or even erosion of the business.

(Link to the Full Article)