

Project Type: White Paper

Details: This white paper comparing the experiences of two companies to explain the benefits of a service that helps organizations protect sensitive data in the test environment.

Excerpt:

INTRODUCTION

This paper presents the experiences of two companies who engaged in test data privacy projects. Both companies are in the financial industry and their non-production environments are of a similar size. They differed in how they scoped the effort surrounding protecting PII in their non-production environments.

Company A took a tactical approach in which they worked with the vendor to ensure the technology was installed correctly, users were trained and a few pilot applications were masked. Once these initial goals were met, they decided to tackle the rest of the project in-house.

Company B used a strategic approach, which took a more holistic view of the enterprise. The strategic approach begins with a formal assessment that provides a high-level test data privacy implementation roadmap for the entire organization.

While both had some success, the company that used the strategic approach had a much better experience. It was able to mitigate risk sooner, had increased visibility into the project at all times (which was critical for executive management) and spent substantially less money in the completion of the project.

This white paper discusses the lessons learned while working with both companies, elaborating on the unique challenges they faced and successes they achieved.

LESSON 1: ALL LINES OF BUSINESS NEED TO BE INVOLVED EARLY.

When starting a data privacy project, the first thing most organizations want to understand is the risk exposure of their sensitive data. This is not an easy task. To get an accurate view, you need to work with multiple lines of business, asking the right questions, collecting the appropriate data and pulling all of the data together in a way that makes it meaningful.

Finding this information was a struggle for Company A. There were no standard processes for the protection of sensitive data, and each line of business had its own procedures. In fact, it was common for individual developers to decide how to handle their own data.

