The site maintains a comprehensive database of data breaches reported in the United States dating back to 2005, providing robust longitudinal data. Researchers could conduct quantitative analyses to identify trends over time, such as whether the frequency or scale of breaches has increased year-over-year, what industry sectors experience the most incidents, the types of vulnerabilities commonly exploited. The level of detail recorded, including organizational impacts, records affected, and reported causes of intrusions, offers researchers qualitative insights. Analysts could examine case studies to understand how and why particular compromises occurred, comparing sophisticated targeted attacks versus major breaches attributable to simple oversight issues. Grouping breaches by variables like time of year, location, company size or technological environment affected may reveal clusters or correlations worthy of further investigative study. For example, determining whether certain jurisdictions or technologies show disproportionate risks.