CASE STUDY

Financial Institution Prepares for GDPR and NYDFS Regulations Using RiskLens

Challenges

With new regulatory mandates on the horizon from GDPR and NYDFS on cybersecurity, executive management was faced with the decision of how to protect its customer data via encryption or an "acceptable" alternative. Could the organization get away with implementing drive encryption throughout, or should they invest in file encryption where this sensitive data is stored?

Solution

Using RiskLens, analysts determined the current exposure to a breach of customer data, including the potential cost of fines imposed by GDPR and NYDFS. Additionally, they determined the amount of risk reduction, in dollars and cents, if either drive level encryption or file level encryption was implemented.

Results

Executive management was empowered by data to make a decision on the type of encryption to invest in that not only allowed them to meet GDPR and NYDFS regulatory requirements, but significantly reduce the amount of risk the organization faced related to protection of customer data.

The Challenge

A global banking and financial services holding company with over $300B in total assets is preparing for the upcoming European Union General Data Protection Regulation (GDPR) and New York Department of Financial Services (NYDFS) cybersecurity regulations. While the depth and breadth of these requirements may differ, their primary message is the same - protect your sensitive customer data, or pay a significant price. Executive management was faced with the decision of how to protect its customer data at rest via a "reasonable" form of encryption that met the legal requirements. Could management just implement drive encryption on its devices, or should they invest in file encryption where this sensitive data is stored? The organization's conventional approach to risk rankings could not support executive management's decision. In order to answer these questions, the organization needed to start communicating risk using the method best understood by business stakeholders: dollars and cents.

The Solution

The RiskLens platform combines an intuitive workflow process for scoping and data collection with a sophisticated analytics engine based on Factor Analysis of Information Risk (FAIR), an industry standard for the quantification of information security risk.

We began by focusing our analysis on the amount of risk associated with a breach of a single database housing approximately 40K records of customer PII data, which was currently unencrypted. The analysts used the simple scoping capability within RiskLens to rapidly determine what data points were necessary for the analysis; effectively reducing their work load by removing research into data that did not ultimately support quantifying risk. The analysis collected data through structured workshop questions on key risk and control factors including historical number of breach attempts, existence of monitoring tools such as database access monitoring and DLP, number of PII records potentially impacted, and resources required to respond to data breaches. The analysis also leveraged industry loss tables to estimate the potential effect a data breach would have on customers and regulators, and adjusted these figures to account for additional fines imposed from GDPR and the NYDFS regulations, using data distributions.

Inevitably the estimates used to calculate risk have a degree of uncertainty associated with them. However, like all data input into the analysis, distributions allow the organization to account for uncertainty. Over the course of a three-day period, the organization was able to efficiently produce both high level reporting and detailed results describing, in financial terms, the effect of a breach of a non-encrypted database containing PII.

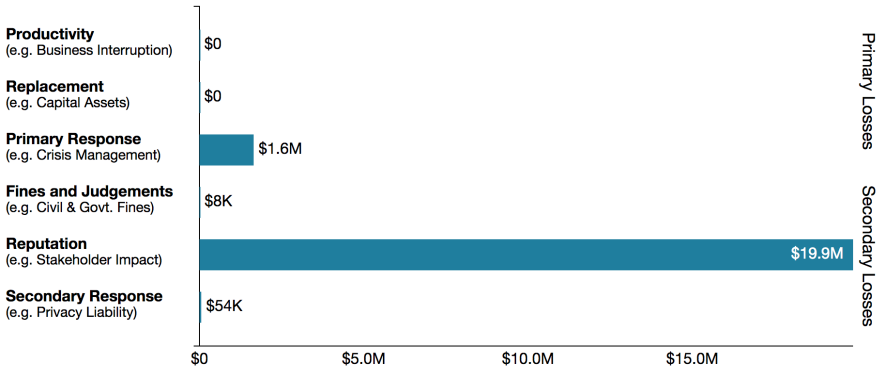


Figure 1: Exposure by FAIR form of loss

Figure 1 clearly illustrates the loss exposure materialized across several categories that incorporate lost revenue due to incident response, regulatory fines, and lost market share due to reputation damage. The tabular data communicated the varying range of probable outcomes.

The powerful versioning capability of RiskLens allows future analyses to be rapidly performed. In this scenario, the analyst leveraged the tool's versioning capability to make several "what if" adjustments to the existing analysis to model risk in the event that drive encryption or file encryption were implemented on the given database. These comparison reports provided the organization with tangible data to make a decision on the type of encryption to implement. The results were telling – one type of investment clearly outweighed the other in terms of risk reduction.

Key Benefits

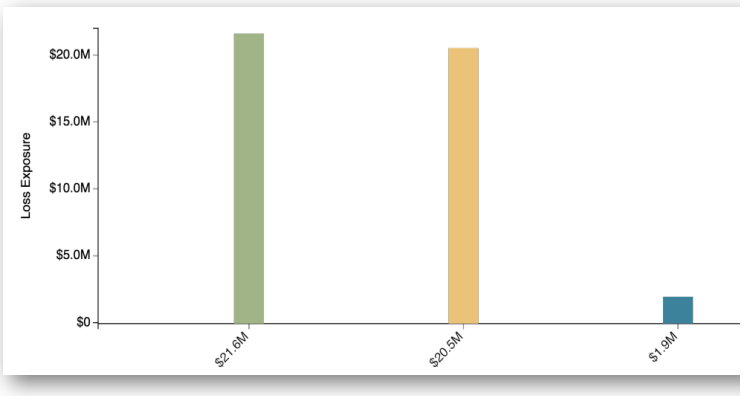
The RiskLens platform allowed the organization to rapidly quantify the loss exposure of a data breach in the event that their PII data was unencrypted. Additionally, the quantitative inputs and documented rationale provided an opportunity to review and challenge the inputs used during the analysis. More importantly, it empowered management with data to make a strategic decision on the type of encryption to invest in to meet the GDPR and NYDFS regulations while maximizing their risk reduction. The organization also discovered that by modifying the record count and re-running the analysis, they could leverage RiskLens to extrapolate the results across the organization to determine the total loss exposure of similar unencrypted databases.

Risk Reduction Drivers of File Encryption

- *Decrease of secondary loss magnitude of a data breach*
- *Decrease of required response efforts, credit card monitoring, reputation damage, etc.*

Figure 2 compares the loss exposure for the current state environment compared to the loss exposure once the two types of encryption were implemented. Combined current state loss exposure (average) was $22M annualized. Implementing drive encryption only slightly decreased the loss exposure by $1M, which was driven primarily by a slight reduction in fines and judgments from regulators. The more significant impact was the $20M risk reduction from implementing file encryption. Of course, the scenario analyzed assumed a breach of a maximum of 40K records. Once this scenario was extrapolated across multiple databases of similar build, the results were truly impactful – a risk reduction of approximately $4.5B in the event of a data breach of 10 million records. For the first time, the analyst team could report results to executive management that were actionable, using a language common amongst all stakeholders.

Figure 2: Loss exposure comparison



No encryption $21.6M, drive encryption $20.5M, file encryption $1.9M)