# Research Synopsis

White Paper Title: Estimating Financial Losses From A Data Breach

Author: Justin Theriot, Senior Data Scientist, RiskLens

Publication date: Oct. 19, 2021

## Research Abstract

- "In the last decade researchers have focused on developing a model to estimate the financial losses a firm will incur after a data breach. Our research asks, can we better estimate financial losses incurred after a data breach by aggregating losses into separate categories and modeling them independently?"
- "Our approach utilized the Advisen data set to estimate losses by separating them into three categories and modeling on the following independent variables: record count, country, threat access, threat type, data type, and industry."
- "Overall, we have provided a multi-faceted model enabling the cyber community to better understand the what, where, and why of financial losses incurred after a data breach."

### THIS RESEARCH COVERS 3 CATEGORIES OF LOSS:

- Primary Response Costs (PRC): "The first loss category is those costs associated with managing the data breach by deploying an incident response team, computer security incident response team or other related teams. These are costs that always accrue after a data breach."
- Fines and Judgments (F&J): "The second loss category includes fines incurred from a regulatory body, judgments in civil cases, or fees paid based on contractual stipulations."
- Secondary Response Costs (SRC): "The third loss category includes a variety of costs related to activities and expenses incurred in dealing with secondary stakeholders, depending on the nature of the data breach."

## Key Findings

### 1. Impact of Record Counts on Loss

The number of records in a breach often (but not always) impacts the costs associated with a breach:

- As the number of records increases by 10%, we can expect PRC to increase by 5.3%.
- As the number of records increases by 10%, the probability of experiencing F&J costs increases by 0.8%.
- As the number of records increases by 10%, we can expect F&J costs to increase by 1.8%.
- As the number of records increases by 10%, we can expect SRC to increase by 2.7%.
- Record counts have no impact on the probability of experiencing SRC.

## 2. Impact of Victim Industry and Data Type on Loss

The victim organization's industry and the types of data the organization holds have an impact on breach costs:

### VICTIM INDUSTRY IMPACT:

- The Healthcare, Information, and Finance industry are 1.5x, 2.0x, and 2.5x, respectively, more likely to experience SRC compared to other industries.
- F&J costs levied against the Finance and Information industries are 1.9x higher compared to other industries.

### DATA TYPE IMPACT:

- Breaches involving protected heath information (PHI) data are 2x more likely to incur F&J costs.
- Breaches involving payment card industry (PCI) data are 3.1x more likely to incur SRC.

## 3. Impact of Type and Origin of Event on Loss

The types of events and origins of those events have an impact on breach costs:

### TYPE OF EVENT IMPACT:

- Malicious events incur 1.4x higher F&J than events caused by an error.
- Malicious events incur 2.0x higher SRC than events caused by an error.

### ORIGIN OF EVENT IMPACT:

- Data breaches due to external actors are 2.4x more expensive than those caused by internal actors.
- Internal events are 40% more likely to experience F&J compared to external events.
- Internal actors see SRC increase by 70% compared to those caused by external actors.

# Implications and Conclusion

Our research provides various applications we all can use in our work today.

First, our estimates are based on industry, geography and data type such that you can develop a loss estimate specific to a company based in the US, in the Healthcare industry, with a given number of PHI records.

Second, better understanding variables can help organizations compare scenarios, to help drive prioritization exercises: For example: should budget increases be allocated to improving internal or external access controls across a set of assets?

Third, since this research separately modeled various costs, this not only improves final estimates, but also facilitates communication with stakeholders enabling us to express to enterprise risk management the total risk of a scenario, as well as accurate decompositions of operational costs vs legal costs.

Lastly, with data driven deployable models, analysts can perform all three of the above tasks without having to consult other departments or attempt to make in-house estimates; they can rely on our work freeing more time to develop solutions for their risk landscape.

In this research, we've helped to illustrate that there is no one-size-fits-all amount of risk for any organization, and instead the entire scope of a FAIR-based scenario, including industry firmographics like those presented here, can dramatically impact expected losses.