CASE STUDY

Finding a Cost-Effective Fix for Employees Leaking Confidential Data by Email

Challenge

The company suspected it was suffering "death by a thousand cuts" from data leaks but couldn't get its arms around the extent of the problem or how to fix it.

Solution

Using RiskLens, the team gathered and made sense of the available GRC data and put hard numbers on the losses.

Results

With solid estimates on costs, the team was able to identify the best vendor solution then make a clear case to management based on meaningful financials.

The Problem

The risk management team at a Fortune 500 financial services company took a good look at its GRC tool and noticed a pattern – from all across the company, which handles large volumes of personally identifiable information, business units were reporting the same problem: release of PII by employees through accidental emailing.

These were minor accidents by well-meaning employees, really. The "type ahead" function would auto-fill the wrong email address and the employee wouldn't notice before hitting send, or the employee would mix data from two clients in one email attachment.

But each incident required a response and remediation: an investigation team had to collect affidavits from the email recipients stating that they had not handled the misdirected data, and the offended owners of the data had to be offered credit monitoring services.

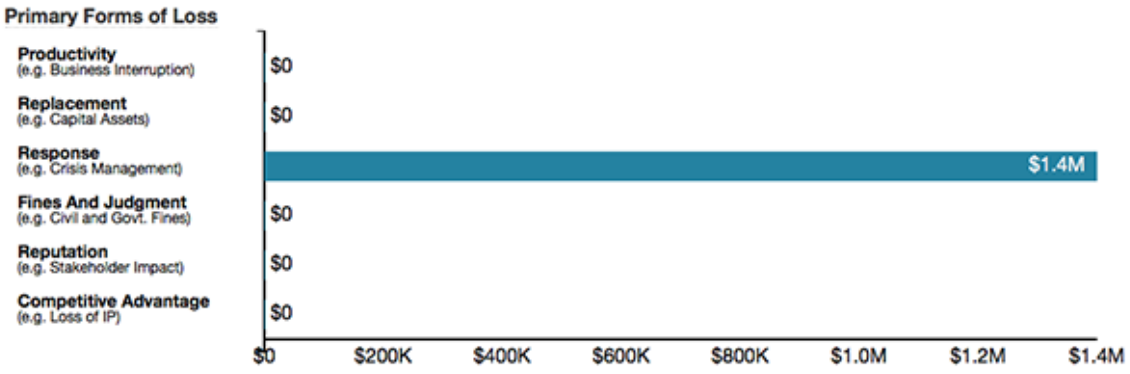
Costs were low per incident but, as the risk team did a quick qualitative triage they realized that the high-frequency, widespread occurrence of the events added up to "death by a thousand cuts," as the risk team leader put it, so "we said let's make it an enterprise operational risk issue and do the quantitative analysis with FAIR and RiskLens."

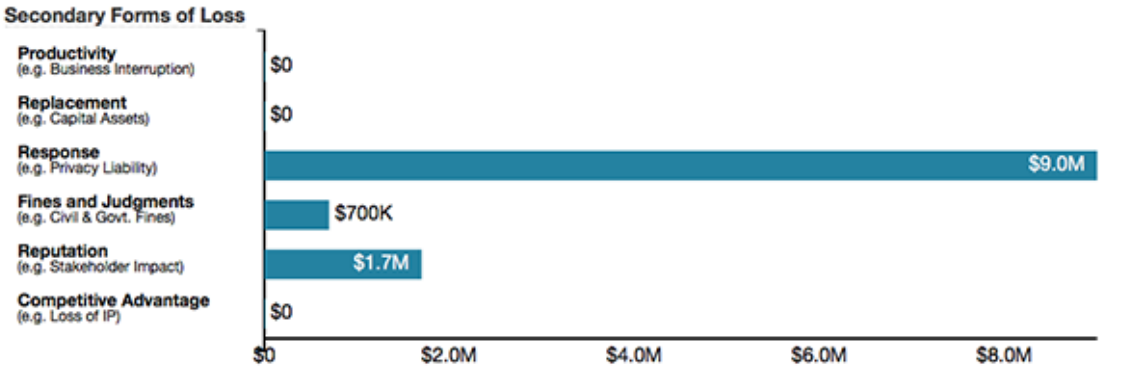
The Solution

With the guidance of RiskLens consultants, the team set out to build their analysis. "We had the raw data in the GRC tool but how we interpreted and used it as input to the FAIR model was key. It took a village to get it right."

The team was able to get a good fix on Primary Response and Secondary Response (the investigation effort, credit monitoring payments, etc.) "but FAIR really helped us get down to the core secondary losses, relating to brand impact and reputation loss, and especially fines and judgements – we had no historical data, so we had to rely on RiskLens to tell us a reasonable number".

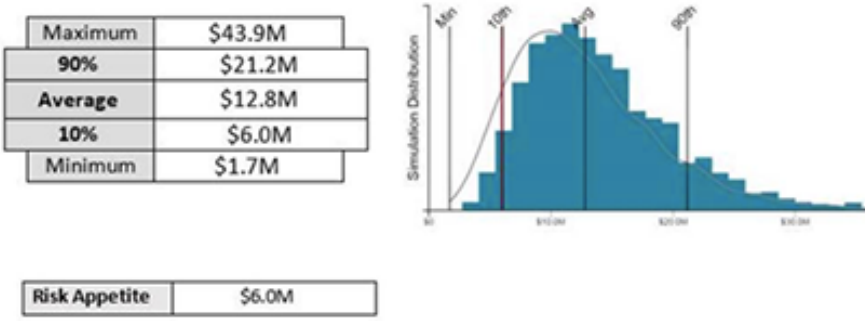
See the **Forms of Loss** chart on the next page.





With the loss data input, the team could run thousands of scenarios using the RiskLens Monte Carlo engine to arrive at a range of estimated outcomes for Aggregate Loss Exposure at an average of $12.8 million.

See the **Aggregate Loss Exposure** chart to the right.



The team next used the RiskLens comparative analysis to see what type of mitigation "would get us the biggest impact in risk reduction". Among the contenders: more training for the staff (already proven ineffective), stop sending emails (a reputation loser with clients), set up a self-service website for clients to retrieve their own files or buy a simple SaaS application that stopped employees each time they attempted to email clients and asked them to double check their message for a wrong address or any improper PII transmission.

Benefits & Results

Between the two serious contenders, the self-service website costed out at more than the loss exposure, while the SaaS application would only cost $120,000 across the enterprise and bring an estimated 38% reduction in risk off the current $12.8 million average. "We presented those numbers to management and the reaction was like: Do it, stat!" says the team leader.

"When you're speaking in the language of the business, dollars and cents, they know what you mean, it doesn't require context, especially when you can describe how those numbers were broken down. They can clearly see the risk reduction and that adds a great deal of credibility for future analyses".