« Return to Blog Listing

4 Steps to Measure Controls' Effectiveness with Cyber Risk Quantification

by *Cary Wise* on *Feb 14, 2019 7:00:00 AM*

I sometimes run into risk quantification fans who are sold on the process but just don't know how to get started. But conceptually, with the FAIR model, quantitative risk analysis has a simple and logical flow, and the RiskLens platform automates the complexity and scale that can make enterprise-level risk quantification difficult and time-consuming.

Here I broke the process down to four simple steps to analyze a question that any organization will face: invest in a control or not (in this case, encryption for a PII database). Try this and you'll be on your way to regularly making informed, risk-based decisions that effectively manage the limited resources of your organization.

1. Identify current risk exposure

To begin evaluating the control investment, you must first understand the current risk exposure related to the scenario without the control in place. For example, if the purpose of the analysis is to assess the risk reduction associated with implementing encryption on a database containing customer PII, the first step would be to assess how much risk is associated with a breach of said database in its current state. Analyzing the current state risk exposure involves a four-step process:

1. Scope the Scenario
2. Gather the Data
3. Run the Analysis, Q/A the Results, Refine the Estimates
4. Report the Results

After you have an understanding of the current state risk exposure, you can assess how the control you are considering would impact the analysis. It is common for people to associate controls with vulnerability and resistance strength, and assume their only benefit is preventing the loss event from occurring, however, using the FAIR model, there are four main control categories:

1. Avoidance
2. Deterrence
3. Resistance
4. Responsive

Each of the above categories maps to a different area of the model and impacts the analysis in a different way.

For more information, see **How to Model Controls in a FAIR Analysis**.

In the example above, encryption would be modeled as a Responsive control as it changes the potential losses you would experience from the event.

3. Perform a future state analysis, evaluating the effectiveness of the control

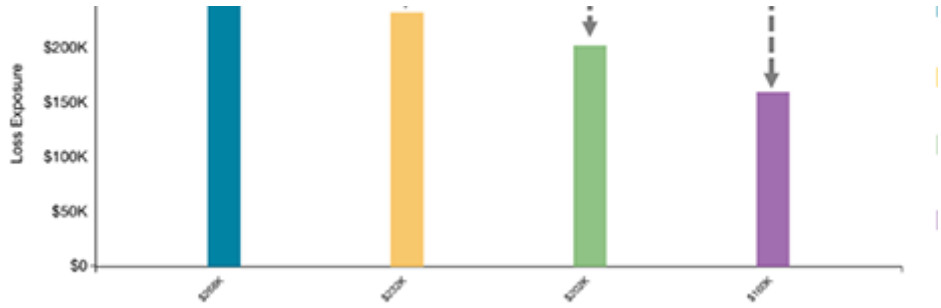
Once you have mapped the control to the FAIR model, the next step is to understand how and to what extent encryption would specifically impact loss exposure. Given that encryption renders the information virtually useless, it would impact the Secondary Loss Event Frequency and reduce the likelihood of additional costs such as notifying customers, fines and judgments, credit monitoring, and reputation damage.

After determining how the control would impact the analysis, you can then version the current state analysis and assess the future state loss exposure with the control in place.

4. Compare the current state vs. future state to perform a cost-benefit analysis

Having completed both analyses, you will be able to see both the current state loss exposure as well as the future state loss exposure with the control improvement taken into consideration. This allows you to determine the reduction in annualized loss exposure, which can then be used to create a cost-benefit analysis for the control investment.

Schedule a Demo



Learn more: What Does RiskLens Reporting Tell Me?

Sign Up for Blog Updates

This post was written by Cary Wise

Cary Wise is a Risk Consultant for RiskLens

Comments

First Name*

Last Name

Email*

Website

Comment*

protected by reCAPTCHA
Privacy - Terms

Submit Comment

Sign Up for Blog Updates

Schedule a Demo

- Instant
- Daily
- Weekly
- Monthly

Submit

Recent Posts

- 4 Ways RiskLens Beats Spreadsheets for FAIR Risk Analysis
- 4 Steps to Measure Controls' Effectiveness with Cyber Risk Quantification
- Case Study: What's the Value of a Data Retention Policy?
- Build Your Career in Risk - Get FAIR-Trained in 2019
- Wall St. Journal Asks: What's the Magic Number for Cybersecurity Budget? We Have an Answer

Popular Posts

- Definitions: Cyber Risk vs. Technology Risk. What's the Difference?
- Monte Carlo Simulation 101 in 5 Minutes [Video]
- Are There Better Alternatives To Heat Maps?
- 4 Steps to a Smarter Risk Heat Map
- SEC Tells Public Companies to Up Their Game in Assessing and Disclosing Cyber Risks

Schedule a Demo

+1 (866) 936-0191

Home

Why RiskLens?

Chief Information Risk Officers
Cyber Risk Management
Legacy Approaches Fall Short
Why Choose RiskLens?
Are You Ready?

Applications

Cyber Risk Quantification
Cyber Risk Triage
Cyber Risk Maturity

Platform

Services

FAIR Training and Certification
Application Training

Resources

Blog
Case Studies
Resource Center
What is FAIR?

Company

What is RiskLens?
Leadership
Newsroom
Events
Careers

Contact

Schedule a Demo