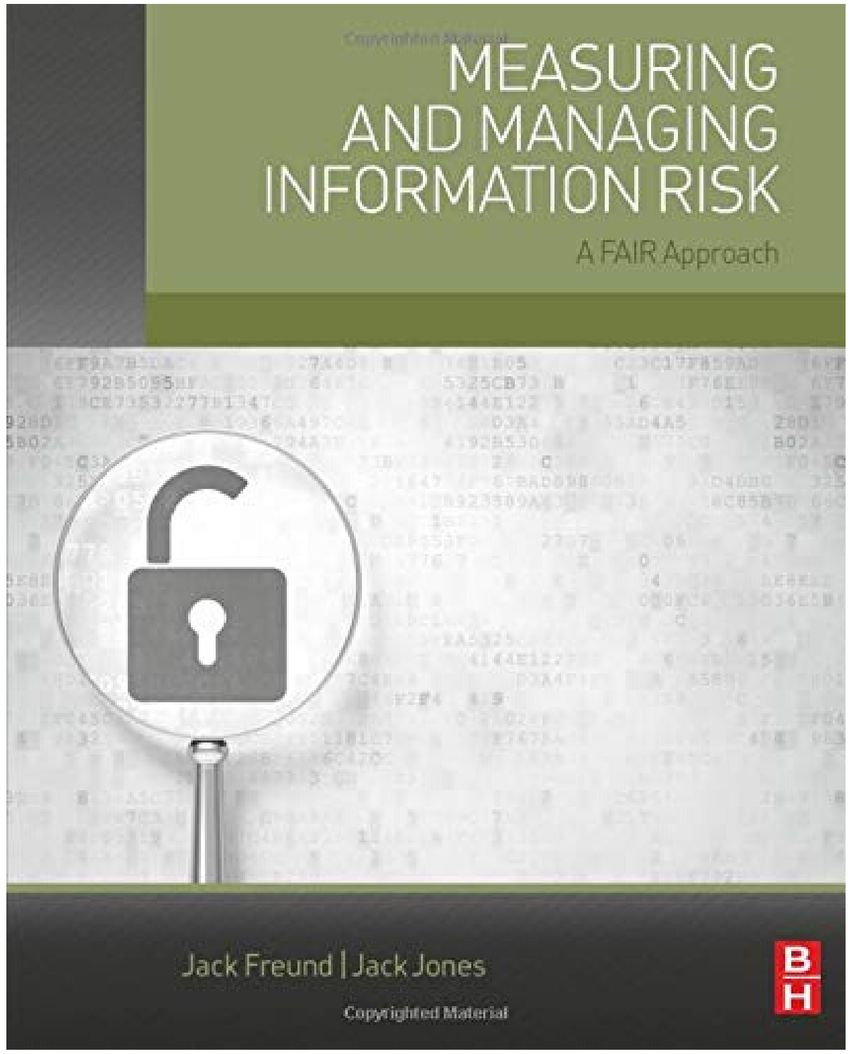
BOOK CLUB

Measuring and Managing Information Risk

Part 1: Chapters 1 - 3



How to Use the Book Club Guide

The guide is meant to drive discussion around the book. Each page will contain information, quotes, and concepts that can be used as topics during your meetings - skip those that may not be relevant and let the discussion flow around those that are impactful - ENJOY!

What Will We Cover Today?

Use the following guide during your book club to drive discussion around the chapters outlined

Chapter 1

Introduction

Chapter 2

Basic Risk Concepts

Chapter 3

The FAIR Risk Ontology

Chapter 1

Introduction - "Warning, this may change your professional life"

1

***Before** reading this chapter - how did you look at risk?*

Did you break out risk as a single risk rating or various decomposition factors (impact/likelihood?

2

Have you been able to effectively answer the question "How much risk do we have" with a risk rating?

What is your biggest frustration with risk ratings?

3

What are you looking to get out of this book?

Answers will differ - but it's best to document as a place to revisit throughout the journey!

The Bald Tire

"Assumptions are unavoidable"

During the 'Bald Tire' example did you confuse things like asset, threat, effect? Even amongst your group did you have different meanings for each? As you make assumptions around what we believe represents each term, did you find there were mixed meanings? Why? What issues do you see with this?

Chapter 2: Basic Risk Concepts

Possibility vs. Probability

Probability vs. Prediction

Subjectivity vs. Objectivitiy

Precision vs. Accuracy

Which concept stands out to you?

What concept does your organization struggle with right now?

How will the idea of possibility vs. probability influence the way you think about risk internally?

Chapter 3: The FAIR Risk Ontology

The secret sauce.

Loss Event Frequency (LEF)

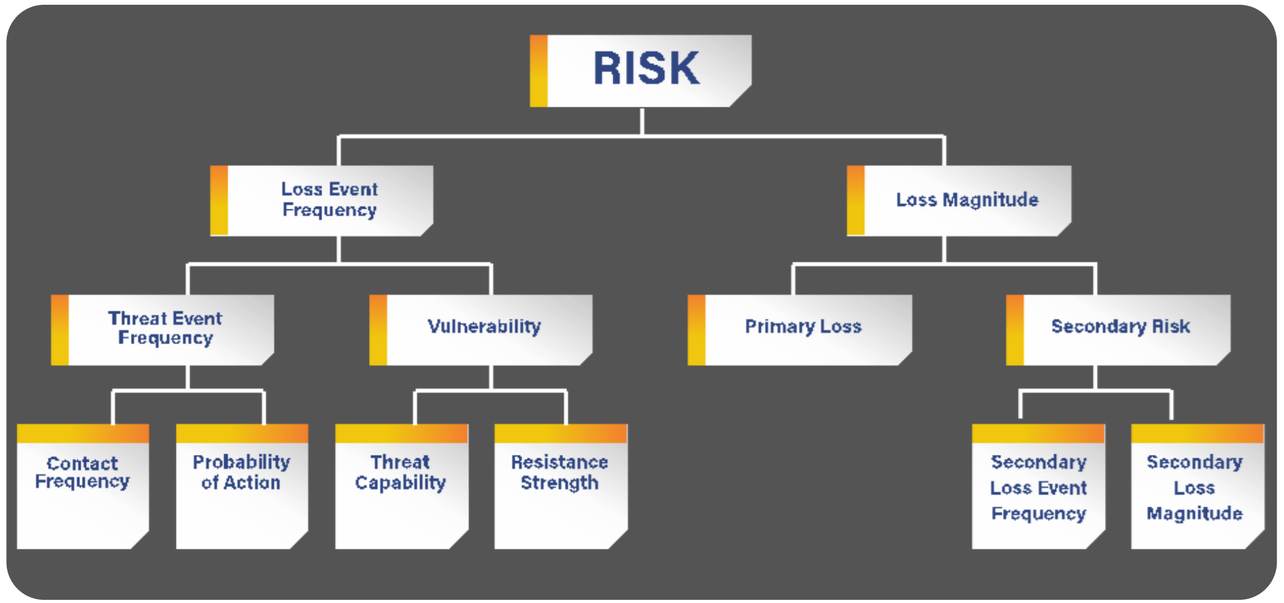
What are some examples within your organization that could represent LEF?

Vulnerability (VULN)

This is one of the hardest 'terms' to adopt because of how we use vulnerability in the InfoSec space currently. How will you begin to measure this variable?

Secondary Magnitude

For your organization specifically, who would be your Secondary Stakeholders?



Final Thoughts?

Open discussion...

Join the Book Club discussion online! Share your club's insights, your feedback to the Guide or pose a question at the FAIR Institute's LINK community site (FAIR Institute membership and LINK signup required).

Join the Book Club discussion online!