

MEASURING AND MANAGING INFORMATION RISK

A FAIR Approach



Jack Freund | Jack Jones



Measuring and Managing Information Risk

A FAIR Approach

Jack Freund and Jack Jones



AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Butterworth-Heinemann is an imprint of Elsevier



Acquiring Editor: Brian Romer
Editorial Project Manager: Keira Bunn
Project Manager: Poulouse Joseph
Designer: Matthew Limbert

Butterworth-Heinemann is an imprint of Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK
225 Wyman Street, Waltham, MA 02451, USA

Copyright © 2015 Elsevier Inc. All rights reserved

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise without the prior written permission of the publisher

Permissions may be sought directly from Elsevier's Science & Technology Rights Department in Oxford, UK: phone (+44) (0) 1865 843830; fax (+44) (0) 1865 853333; email: permissions@elsevier.com. Alternatively you can submit your request online by visiting the Elsevier web site at <http://elsevier.com/locate/permissions>, and selecting Obtaining permission to use Elsevier material

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data

Application submitted

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN: 978-0-12-420231-3

For information on all Butterworth-Heinemann publications visit our web site at <http://store.elsevier.com/>

This book has been manufactured using Print on Demand technology. Each copy is produced to order and is limited to black ink. The online version of this book will show color figures where appropriate.



Both are reasonable arguments. Our point is that it is easy to make assumptions in risk analysis. In fact, assumptions are unavoidable because the world is infinitely complex.

That is our first point—assumptions are unavoidable. Assumptions are also the most likely source of problems within most analyses because, too often, people do not examine their assumptions or even recognize when they are making them. They just shoot from the hip. “That scenario is high risk!” they’ll say. Unfortunately, the person next to them may be making a different set of assumptions and react with, “Are you nuts? Clearly that scenario is low risk!” Most of the time, the disagreement is based on different assumptions.

One of the significant advantages to using FAIR is that its ontology and analysis process help you to identify and clarify your assumptions. That way, when someone questions your results, you are in a position to explain the assumptions underlying the analysis.

TERMINOLOGY

Our second point is that from any group going through the Bald Tire scenario, we will typically get several different descriptions of what constitutes the threat, vulnerability, and risk within the scenario. We’ve heard the frayed rope described as threat, vulnerability, and risk. We have also heard the cliff and rocks described as threat and risk.

The simple fact is that much of the risk profession (including the operational risk discipline) has not adopted standard definitions for these terms. Compare this to other professions. Physicists do not confuse terms like mass, weight, and velocity, and financial professionals do not confuse debit and credit—even in informal discussions—because to do so significantly increases the opportunity for confusion and misunderstanding. It also makes it tough to normalize data. This is important to keep in mind when we’re trying to communicate to those outside our profession—particularly to executives who are very familiar with the fundamental concepts of risk—where the misuse of terms and concepts can damage our credibility as professionals and reduce the effectiveness of our message. After all, our goal is not to create a secret risk language that only we can talk about—effectively isolating ourselves from other risk professionals.

TALKING ABOUT RISK

Go to your local bookstore or library and pick up two different books on risk by two different authors. There is a very good chance that you will find that they have used foundational terminology differently from one another. For that matter, there’s a decent chance that each author uses fundamental risk terminology inconsistently within his or her own book.

So, what are the threat, vulnerability, and risk components within the Bald Tire scenario? The definitions themselves are described in Chapter 3, but within this scenario:

- The threat is the earth and the force of gravity that it applies to the tire and rope.
- The frayed rope introduces some amount of vulnerability, but is NOT a vulnerability itself. Huh? Vulnerability (in FAIR) is a probability statement. In other words,

it is the probability that a threat event (e.g., the force of gravity on the tire and rope) will become a loss event (e.g., the rope breaks). In FAIR, we use the term vulnerability in a way that answers the question, “How vulnerable are we?” In answer to that question, a FAIR practitioner may answer something like, “between 30 and 45%.” Simply stated, the rope represents a control, and its frayed condition simply increases the probability of a loss event. If this still doesn’t entirely make sense to you, it will later as we get into the framework in more detail.

- What about risk? Which part of the scenario represents risk? Well, the fact is, there isn’t a single component within the scenario that we can point to and say, “Here is the risk.” Risk is not a thing. We can’t see it, touch it, or measure it directly. Similar to speed, which is derived from distance divided by time, risk is a derived value that represents loss exposure. It’s derived from the combination of factors described in FAIR’s ontology.

Having made an issue of terminology, the following paragraphs introduce and briefly discuss some basic definitions.

THREAT

A reasonable definition for threat is anything (e.g., object, substance, human, etc.) that is capable of acting in a manner that can result in harm. A tornado is a threat, as is someone driving a car, as is a hacker. The key consideration is that threats are the actors (a.k.a., “agents”) that can cause a loss event to occur. This is in contrast to some common usage, where conditions may be referred to as threats. For example, someone might refer to a puddle of water on the floor as a “threat,” when in fact it is not. It is passive, inanimate, and not an actor in any meaningful way. A person stepping on it is the threat actor. The water simply increases the probability that the threat action (stepping on the wet floor) results in a loss event (a slip and fall accident).

VULNERABILITY

Although the word “vulnerability” is commonly referred to as a “weakness that may be exploited by a threat,” that isn’t how we view things in FAIR. Similar to the term risk, vulnerability is considered a value rather than a thing. As a result, you can’t point to something and say, “Here is a vulnerability!” What you can do is point to a control (like a frayed rope) and declare, “Here is a condition that increases our vulnerability.” It may feel like a fine point, but trust us, it is a critical distinction. The relevance of this distinction will become clearer as you progress through this book.

RISK

The following definition applies regardless of whether you are talking about investment risk, market risk, credit risk, information risk, or any of the other common risk domains:

Risk—The probable frequency and probable magnitude of future loss.

In other words—how often losses are likely to happen, and how much loss is likely to result. Rest assured, we'll get into much more detail on this in Chapter 3.

THE BALD TIRE METAPHOR

In large part, risk management today (particularly operational risk management) is practiced as an art rather than a science. What is the difference? Science begins by analyzing the nature of the subject—forming a definition and determining the scope of the problem. Once this is accomplished, you can begin to form and then substantiate (or not) theories and hypotheses. The resulting deeper understanding provides the means to explain and more effectively manage the subject.

Art, on the other hand, does not operate within a clearly defined framework or definition. Consequently, it isn't possible to consistently explain or calculate based upon an artistic approach. In fact, it doesn't even seek to explain. It just "is." A useful example is shamanism. The shaman rolls his bones or "confers with his gods." He then prescribes a remedy based upon what his ancestors have passed down to him (analogous to "best practices"). Now, some shamans may be extremely intuitive and sensitive to the conditions within a scenario and may be able to select a reasonable solution on most occasions. Nevertheless, the shaman can't rationally explain his analysis, nor can he credibly explain why the cure works (or sometimes doesn't work). In addition, while we would like to believe that best practices are generally effective (as we strive to reuse what we think has been successful in the past), this can be a dangerous assumption. Best practices are often based on long-held shamanistic solutions, tend to be one-size-fits-all, may evolve more slowly than the conditions in which they are used, and can too often be used as a crutch—e.g., "I can't explain why, so I'll just point to the fact that everyone else is doing it this way."

There is, however, no question that intuition and experience are essential components of how we do our jobs. The same is true for any profession. Yet these alone do not provide much traction in the face of critical examination, and are not strong formulas for consistency.

In order for the risk management profession to evolve, we have to begin to approach our problem space more rigorously and scientifically (note that we did not say "purely scientifically"). This means we have to seek to understand why and how, we have to measure in a meaningful way, and we have to be able to explain things consistently and rationally.

RISK ANALYSIS VS RISK ASSESSMENT

Many people don't differentiate "assessment" from "analysis," but there is an important difference. From a FAIR perspective, risk analysis is often a subcomponent of the larger risk assessment process.