
RSA
LETS BE FAIR
THE PATHS TO INTRODUCING FAIR INTO ORGANIZATIONS
Chris Patteson - RSA
1
BUSINESS-DRIVEN SECURITY™

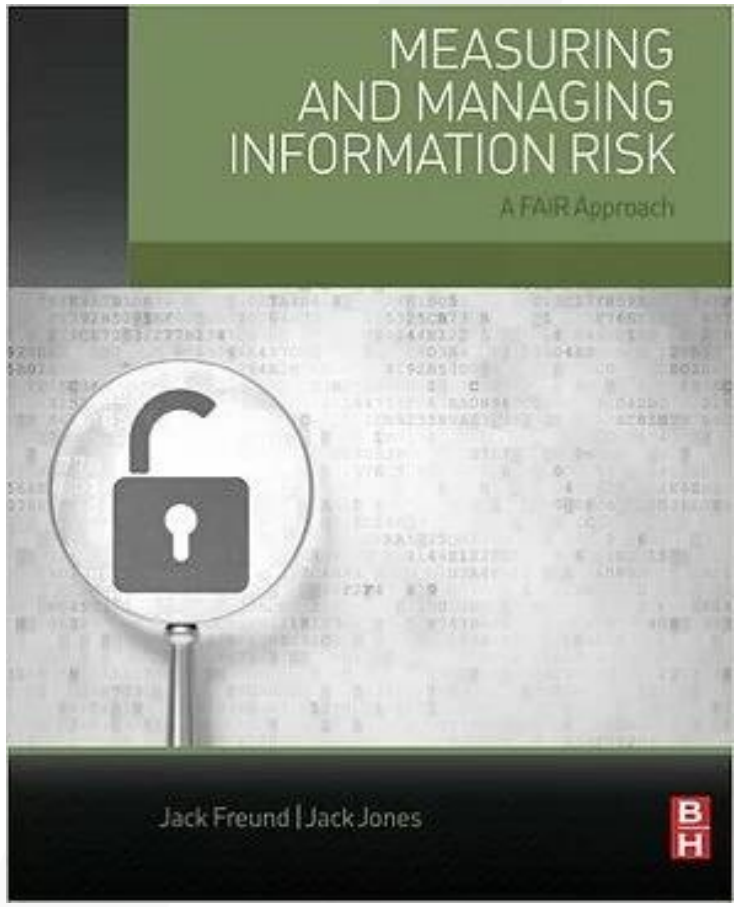

© Peter Bacsfalusi


GREGORY
© Peter Bacsfalusi

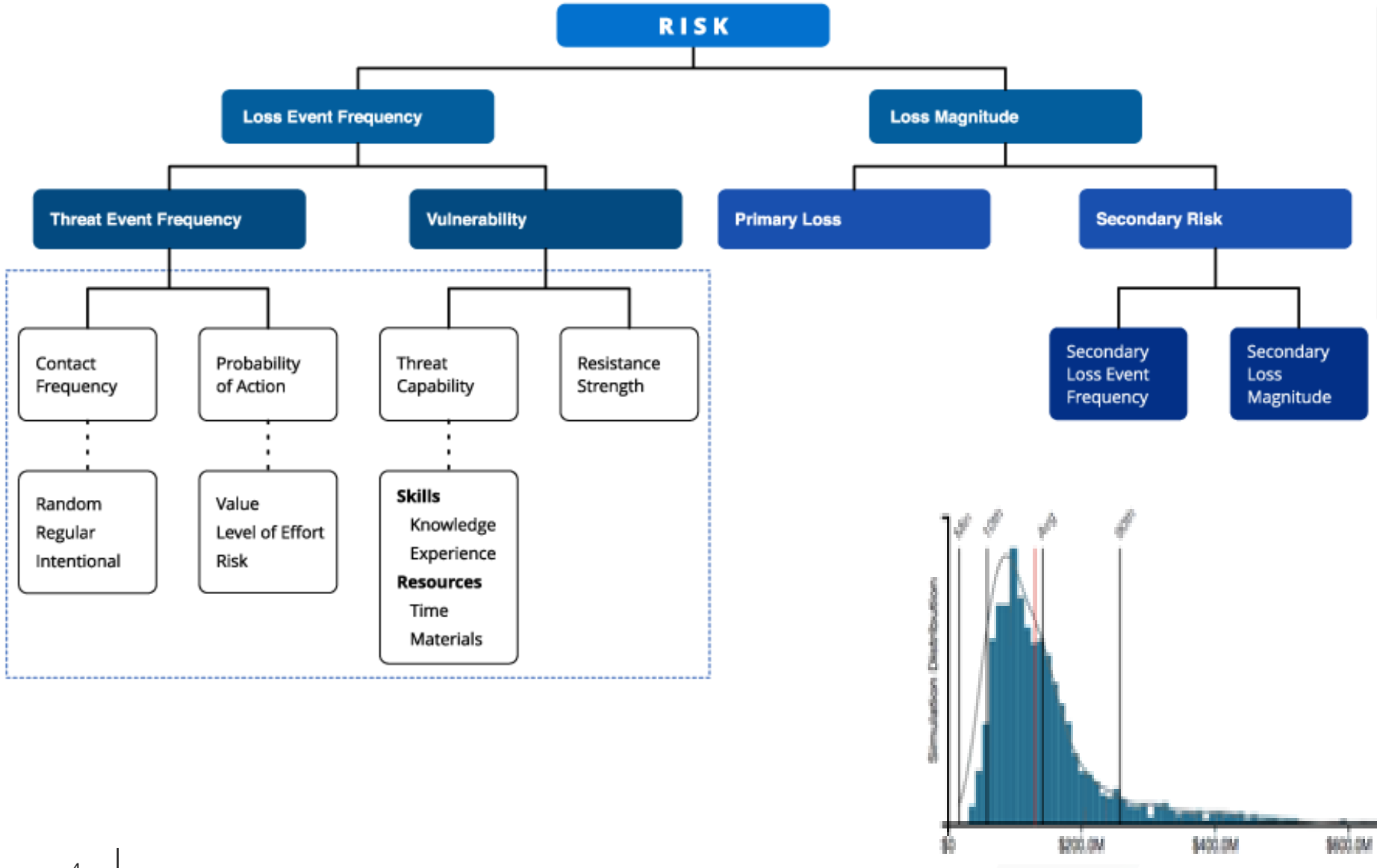
WHAT IS FAIR?

Factor Analysis of Information Risk (FAIR) is the only international standard quantitative model for information security and operational risk.

- FAIR provides a model for understanding, analyzing and quantifying information risk in financial terms.
- It is unlike risk assessment frameworks that focus their output on qualitative color charts or numerical weighted scales.
- It builds a foundation for developing a robust approach to information risk management.



RSA



WHAT DOES IT TAKE TO CHANGE THE WORLD?

Columbus was granted an audience with the monarchy; on May 1, 1489, he presented his plans to Queen Isabella, who referred them to a committee. They pronounced the idea impractical, and advised the monarchs not to support the proposed venture.

WHY ARE WE EVEN TRYING?

We are the visionaries, the problem solvers, answer seekers we want to find a better way!

- Boards are realizing that CyberSecurity poses real risk to their organizations, and pressuring teams for improved quantification. “The rest of the company operates on ROI, where is yours?”
- Information Security teams are failing to deliver?
  - Lack of Budget
  - Targeting the wrong risks
  - Only putting checks on checklists (Frameworks are just a map!)
- Audit and Information Security are looking to adjust their posture in light of rapidly advancing threats
- We have so many 3rd Parties involved in our business we need to evaluate the risk they pose to core operations
- Digital Transformation is underway and improve risk quantification will improve how we manage “Digital Risk” in emerging models

RISK QUANTIFICATION MATURITY JOURNEY

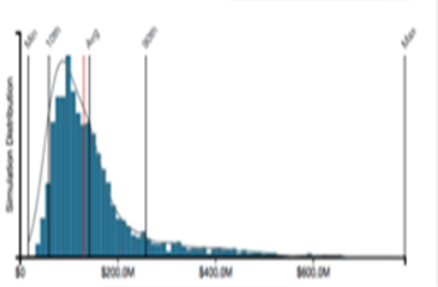
Emerging

Ad-Hoc

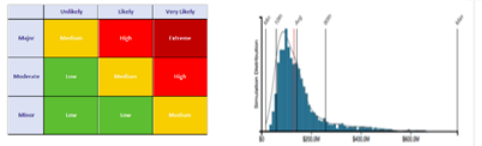
Spreadsheet Analysis

	Unlikely	Likely	Very Likely
Major	Medium	High	Extreme
Moderate	Low	Medium	High
Minor	Low	Low	Medium

Risk Register Matrix (H/M/L)



Risk Modeling (e.g. FAIR, Actuarial, Bowtie)



Dynamic Risk Modeling

Increasing Targeting, Precision, Automation, Complexity =
Reduction of Risk and Control Overlap

RSA

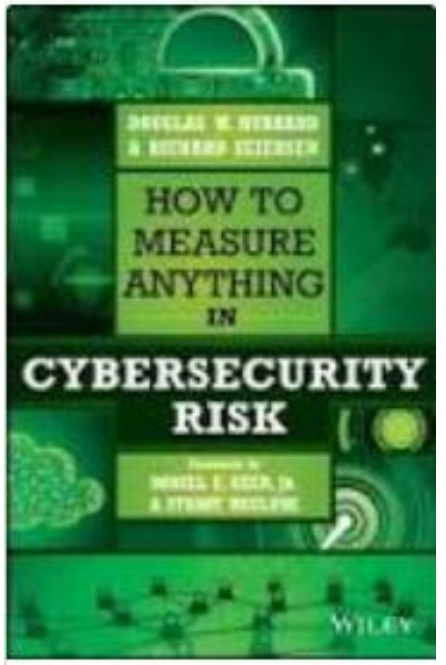
SIDEBAR
HOW THE RISK MATRIX DOES NOT ADD UP

"Stop the Math Abuse" – Carl Conrad, Chevron FAIRCON 2017

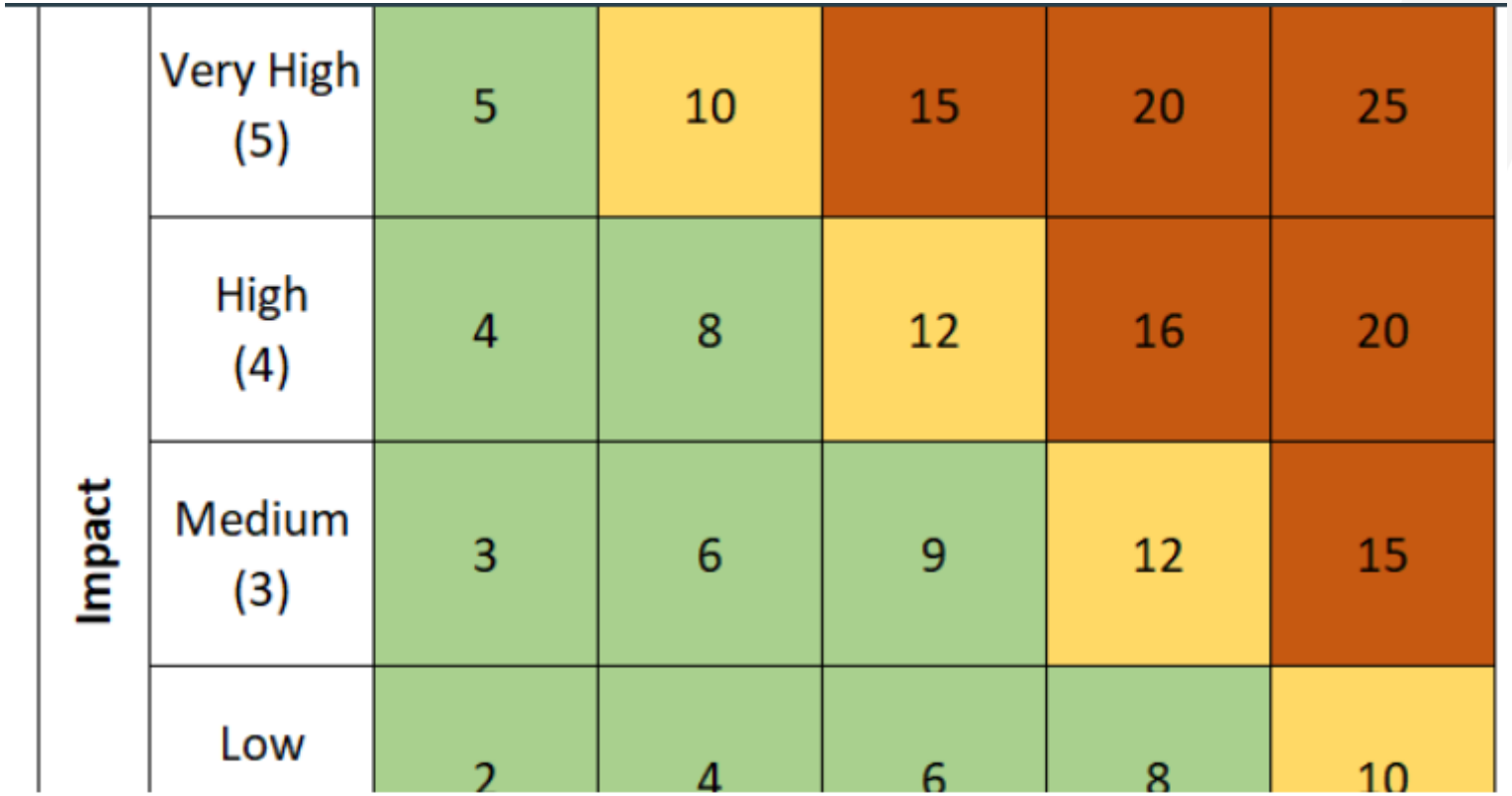
- Risk Acceptance Inconsistency
- Range Compression
- Centering Bias
- Category Driven Bias
- Ranking Reversal
- Instability due to Categorization
- Relative Distance Distortion

The motivation for writing this paper was to point out the gross inconsistencies and arbitrariness embedded in RMs. Given these problems, it seems clear to us that RMs should not be used for decisions of any consequence.

"*The Risk of Using Risk Matrices*"
Philip Thomas
Reidar Bratvold
Eric Bickel



Chapter 5 - Doug Hubbard
Risk Matrices, Lie Factors, Misconceptions and Other Obstacles to Measuring Risk



Impact						
	Very High (5)	5	10	15	20	25
	High (4)	4	8	12	16	20
	Medium (3)	3	6	9	12	15
	Low	2	4	6	8	10

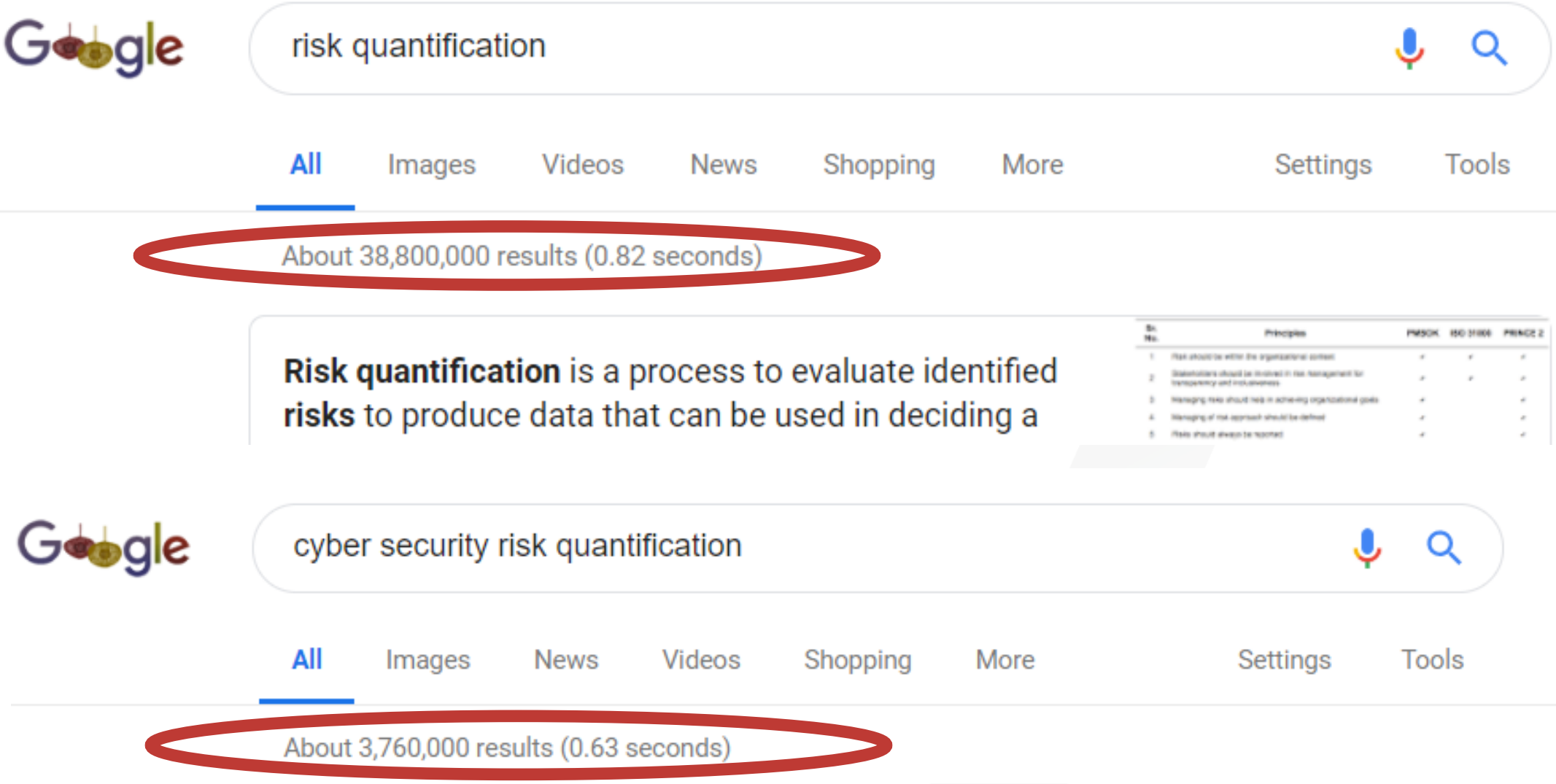
In defence of Risk Heat Maps

Published on January 18, 2019

David Vose | ✓ Following
Risk management expert, author, consultant.
Exec Director of Vose Software
22 articles

885 230 128

RSA



RSA

WHY FAIR?

Open source – The Open Group

Provides and Ontology that can be used with the business

Can operate “with very limited data”

Mathematically / Statistically sound

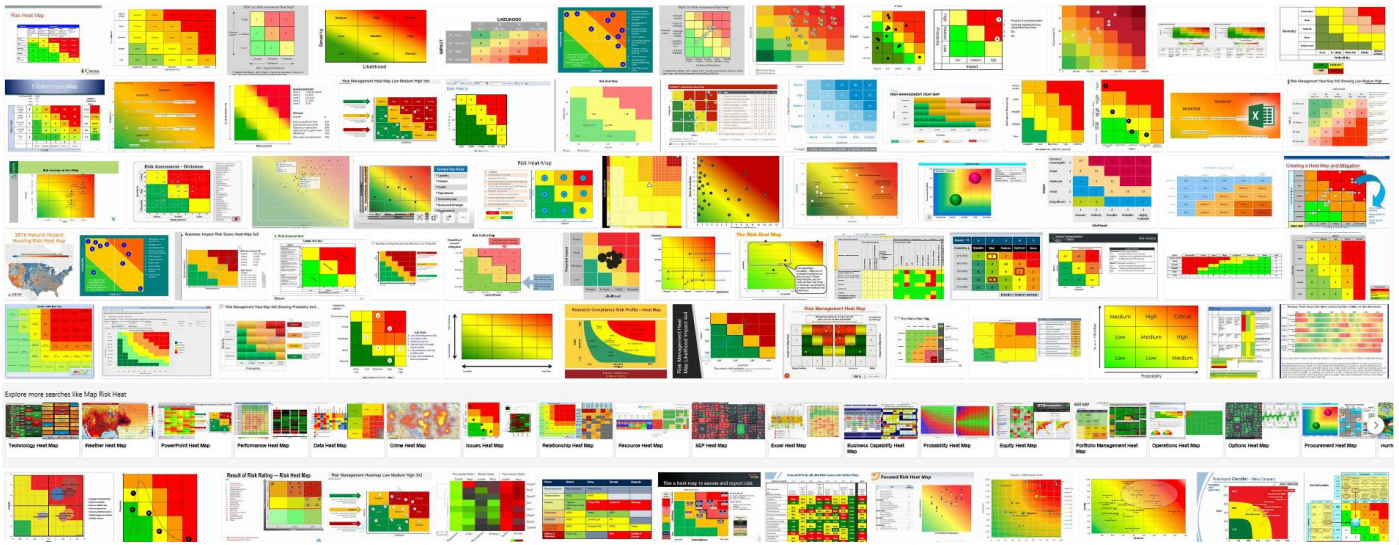
Concepts:

Precision vs Accuracy

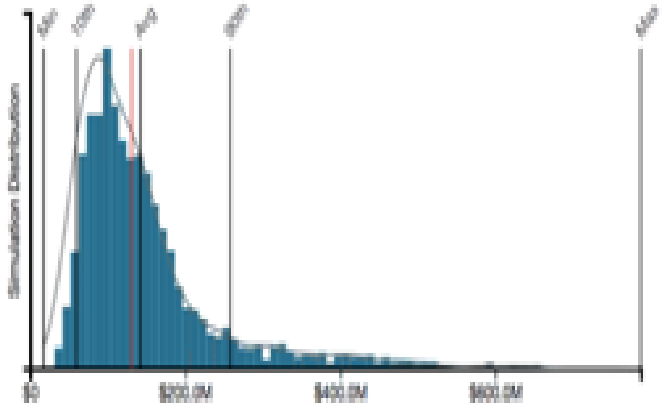
Possibility vs Probability

Subjectivity vs Objectivity

FINDING YOUR WAY



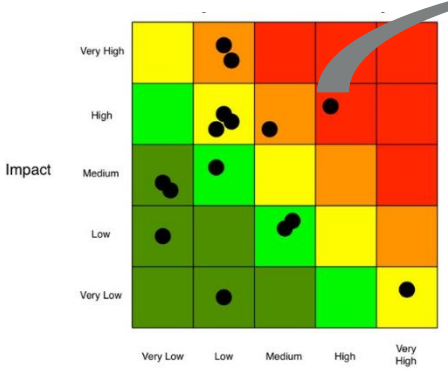
- Easy to understand
- Well entrenched
- Years of careers, investment and decisions
- It ain't broke don't fix it
- Less accountability

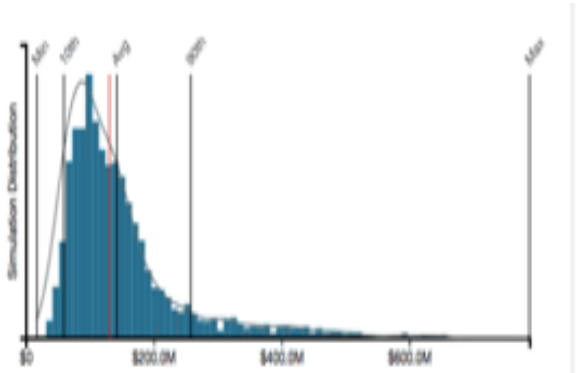


- New and appears complex
- How does it fit into current methodologies?
- Everything else we have is wrong?
- Higher stakes – accountability
- Liability fears

APPROACH 1 – PICK A TARGET AND GO

Risk Register Driven





Executive Driven

Help me really understand what the risk with this new launch is? I need you to quantify this better.

RSA

ARE YOU SETTING YOURSELF UP FOR MUTINY?

RSA

THE PROS AND CONS OF APPROACH 1

- It is a very direct and easy way to start using the methodology
- Has best success when there is full buy in from risk organizations that FAIR should be an organizational standard
- Exposing your vision / position before the culture is ready?
- Methodology is dismissed before it can scale?
- Challenges with aligning with other silos, no common ontology
- Single or very few initial points of reference

RSA

APPROACH 2 – BUILD A FAIR BASED RISK CULTURE

Are These Risks?
Cloud Computing
Insider Threat
Network share containing sensitive information
Mobile Malware
Social Engineering / Phishing
Organized Crime
State Sponsored Attacks
Hacktivists
Ransomware
Internet of Things
Insecure Passwords

Risk = Probability x Magnitude

NONE OF THEM ARE!

STEP 1 CENTRALIZE AND NORMALIZE YOUR RISK REGISTER

For each risk in a risk register:

- Can you estimate Loss Magnitude in $?
- Can you assign some probability (will happen in next 3 months, year, 5 years, 10 years)?

If not….these are likely not risk they could be:

- Inputs for the estimations above
- An Asset
- A Threat Actor or Community
- An attack vector
- A missing control or control failure
- A technology

RSA

PREPPING YOUR RISK REGISTER

- The following fields should be mandatory in the risk register and any risk intake forms
  - Scenario Description (containing threat entity/community, threat type(s), asset(s) at risk, effect)

    In Archer this would likely be a cross reference to allow the scenario to be associated to multiple risks and treatments
  - Loss Freq Range values list (intervals)
  - Loss Freq justification/logic – What support does the practitioner have for this estimation

  - Loss Magnitude Range values list (intervals)
  - Most Likely Loss in $
  - Loss Mag justification/logic – What support does the practitioner have for Loss Magnitude estimations

  - Calculated Risk Exposure - Risk Exposure = Probability x Most likely
  - Calculated Risk Score - Risk Score = log(Risk Exposure*1M)

  These risks can now be plotted in a heat map, and further they can be stack ranked using the calculated Risk Score based on most likely estimation

RSA

WHAT DOES THIS LOOK LIKE?

Probability	$ Event / Likelihood	Severity: Negligible < 10K	Minor 10k ≥and<100k	Moderate 100k ≥ and <1M	Significant 1M ≥and<100M	Severe ≥ 100M
	Very Likely ≥ 10 / yr	Low Med	Medium	Med Hi	High	High
	Likely Once a yr	Low	Low Med	Medium	Med Hi	High
	Possible ≥ 1 and <5 yrs	Low	Low Med	Medium	Med Hi	Med Hi
	Unlikely ≥ 5 and <10 yrs	Low	Low Med	Low Med	Medium	Med Hi
	Very Unlikely ≥ 10 years	Low	Low	Low Med	Medium	Medium

Severity	Range	Value
Negligible	< 10 K	.00005
Minor	10k ≥and<100k	.0001
Moderate	100k ≥ and <1M	.001
Significant	1M ≥and<100M	.01
Severe	≥ 100M	1
Likelihood	**Range**	**Value**
Very Likely	> 10 times a year	10
Likely	Once a Year	1
Possible	≥ 1 and <5 yrs	.2
Unlikely	≥ 5 and <10 yrs	.1
Very Unlikely	≥ 10 years	.05

Risk Exposure = Probability x Most likely

Risk Score = log(Risk Exposure*1M)

An additional field should be created where the user selects the most likely Loss Magnitude in the selected range based on their best estimate. This is the value that should be used in the equation.

SO WHAT HAVE WE ACCOMPLISHED THUS FAR?

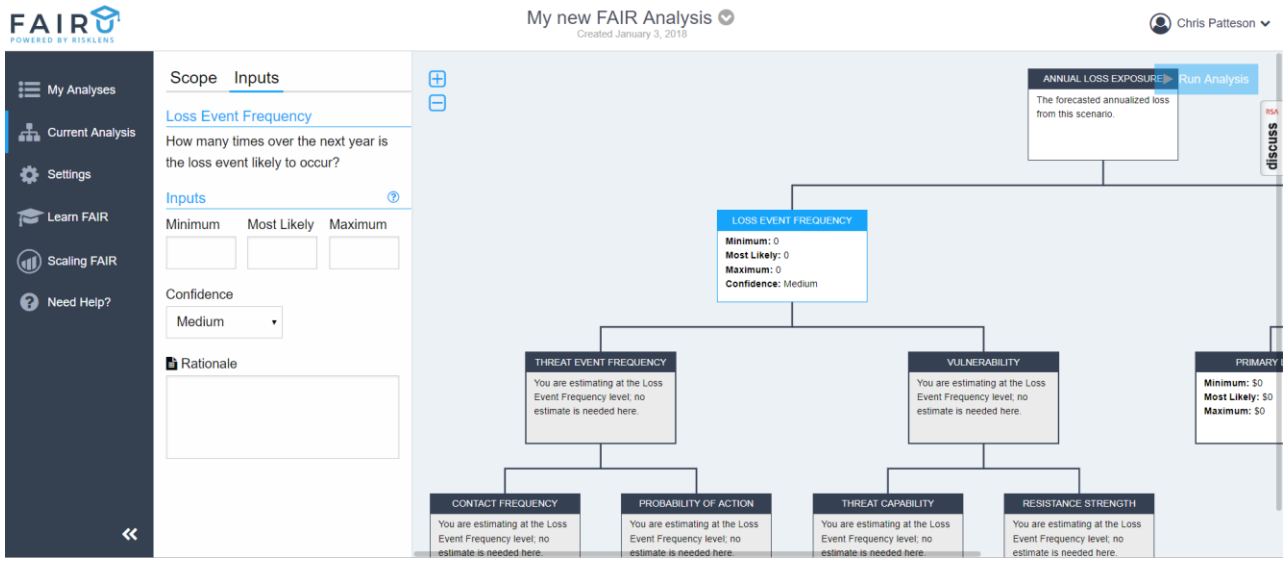
- We are still using the beloved Heat Map and a traditional risk ontology (magnitude and probability)
- 1st and 2nd line are now working on risk based on a common ontology that ties also to FAIR
- The Risk Register has been triaged to contain “true risks” (magnitude and probability)
- Teams are starting to do estimation as they attempt to derive the loss magnitude and frequency
- Those estimates may start debates which starts to open up the opportunity to start calibrated estimation
- You have probabilities, min / max and most likely numbers for modeling
- By having team members define the logic behind their estimations the 2nd line is building up a list of potential data sources for the organization to use in FAIR analysis

RSA

STEP 2 - WADE INTO FAIR

- FAIR Champions should already be familiar with the free tools

FAIR
POWERED BY RISKLENS



The Open Group
The Open FAIR™ Risk Analysis Tool

RSA

STEP 2 - WADE INTO FAIR

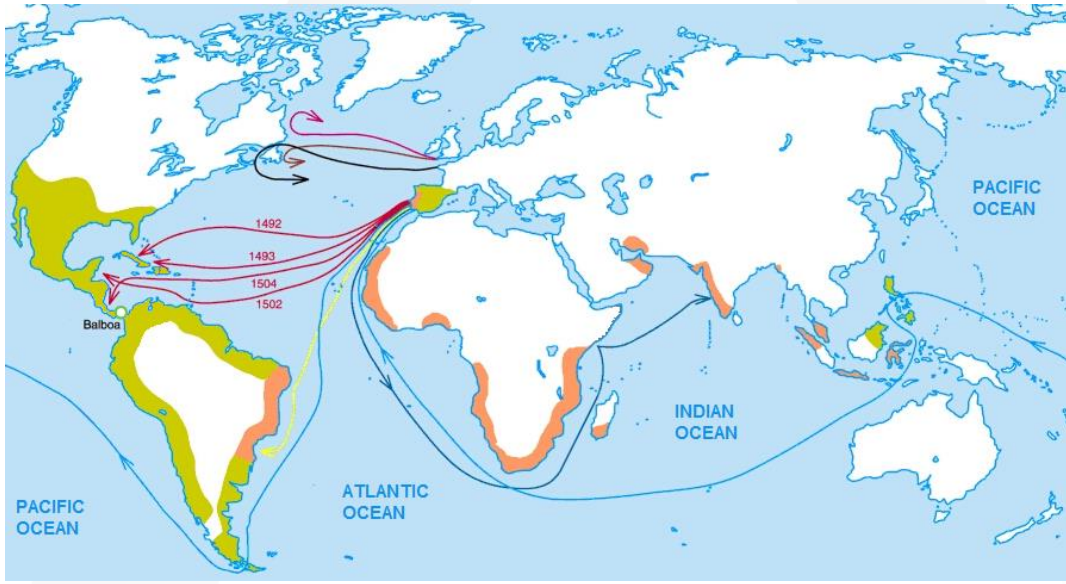
- Caution…..
- This is a “tipping point”
- Non-trained and non certified users need to be careful with how they perform calibrated estimations and feed data into the deeper levels of the models.

- Use the Free tools to start modelling just the first level of the model (wading in)
- This should be done in conjunction with FAIR pilot programs and training
- The initial ranges from the risk register can be used
- Users can break out of the fixed intervals / ranges
- Users can begin enhance understanding of reading the distributions
- Results can be manually loaded into Risk Registers

RSA

THE JOURNEY THAT NEVER ENDS.....

- Centralize more forms of risk into your common register
- Improve collection of new risk from across the organization
- Continue to build depth to scenarios for various risk
- Add triggers for updating of models (what would cause a need to revaluate)
- Seek data sets that can improve precision of your estimates
- Use FAIR to step out of Cyber into other risk domains
- What is your roadmap for scalability?



RSA

START YOUR VOYAGE

- Lock in on the definition of Risk, gain executive support
- Adjust and start normalizing your risk register
- Drive awareness
- Start with basic estimations of probability and loss
- Start developing a bench of expertise
- Be prepared to wade into FAIR appropriately
- Watch for the tipping points

THANK YOU

CHRIS PATTESON –
CPAT@RSA.COM

FAIR INSTITUTE

RSA