Crystal Balls, Tarot Cards, and Other Information Risk Tools

Presented by:

Jack P. Healey, CPA, CFF, CFE, CRISC

CEO

Bear Hill Advisory Group

August 16-18, 2021

GW GEEK WEEK ISACA Atlanta

Our Speaker today

Bear Hill Advisory Group is a boutique consulting firm with a decade of experience helping management teams and their boards understand their businesses better.

Services include business risk assessments, risk incident response plans, interim CFO services, and business process improvements.

Our goal is to help you manage your business of today while building for your business of tomorrow.

Jack P. Healey, CPA, CFF, CFE, CRISC
Chief Executive Officer, Bear Hill Advisory Group, LLC

Jack is an expert in operational, financial and organizational management, strategies, and tactics. He is an expert in risk management, including business risk, risk agility and resiliency, information security risk, and insider threat programs.

He is a Certified Fraud Examiner, Certified Public Accountant, Certified in Fraud and Forensics, Certified Information Systems Controls, Cybersecurity SOC, and Cybersecurity Services. He is a member of ACFE, InfraGard, ISACA , AICPA, RM, and NACD.

He authored the Business Crisis Diagnostic and Prevention Model™, which provides businesses with the framework necessary to identify impending business crises before they occur. He has authored or co-authored articles on Velocity of Risk and Customer Experience.

What is this Presentation all about?

We're here to look at Risk Management in a different light.

Experience has taught that many organizations 'go through the motions' of Risk Management.

Are we really 'managing risk' or are we 'checking the box'?

We're going to draw parallels to Social Engineering/Cold Reading to question-

Is your approach to Risk Management based in reality or an illusion?

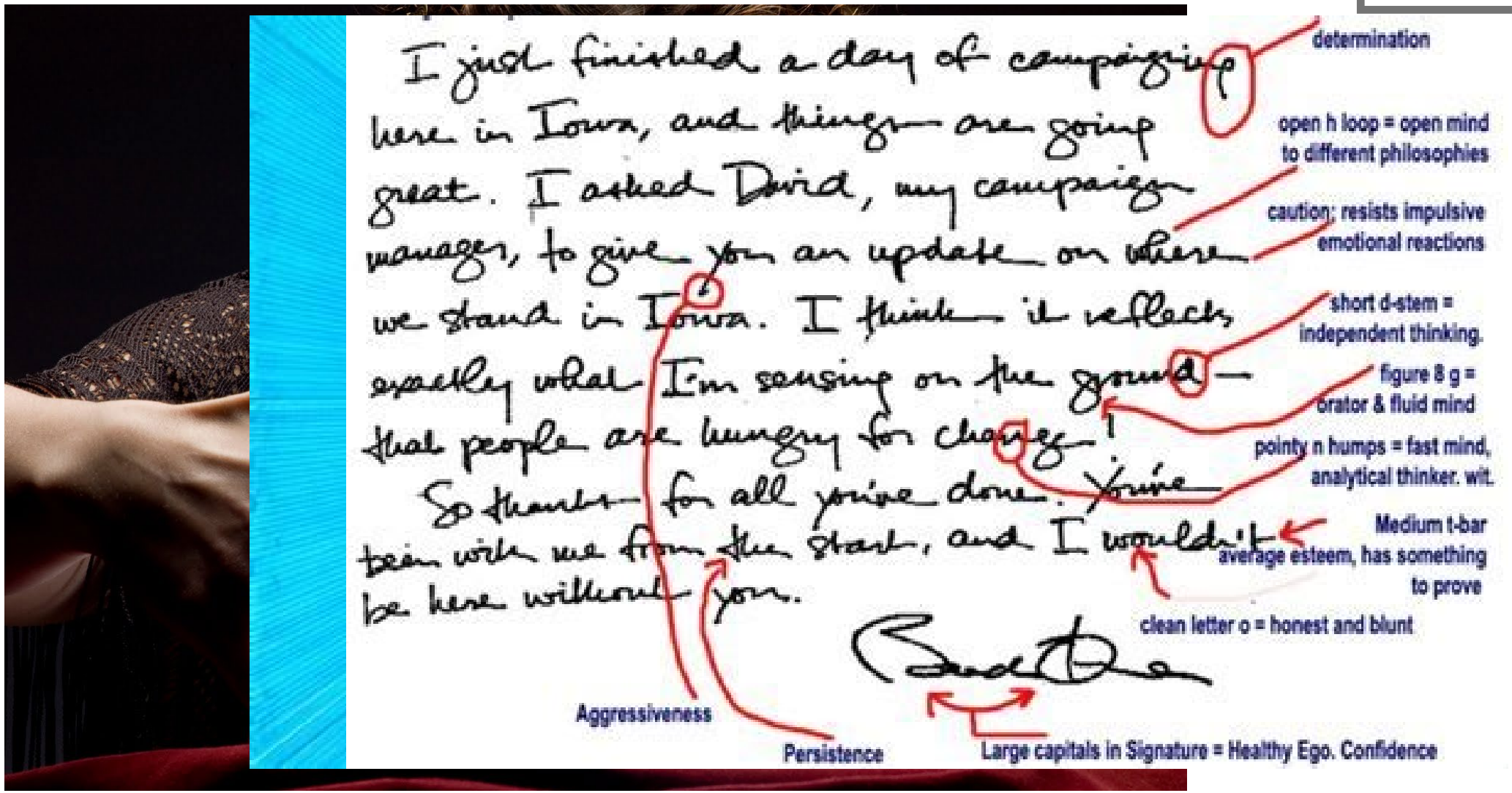
Presentation Road Map

- Cold reading 101
- Navigating the risk management frameworks
- Probable versus possible – why it matters.
- How to overcome functional bias.
- Time and velocity impact on risk management.
- Risk granularity – the key to better risk management
- The often-overlooked relationship between primary and secondary risk
- Tarot card reading

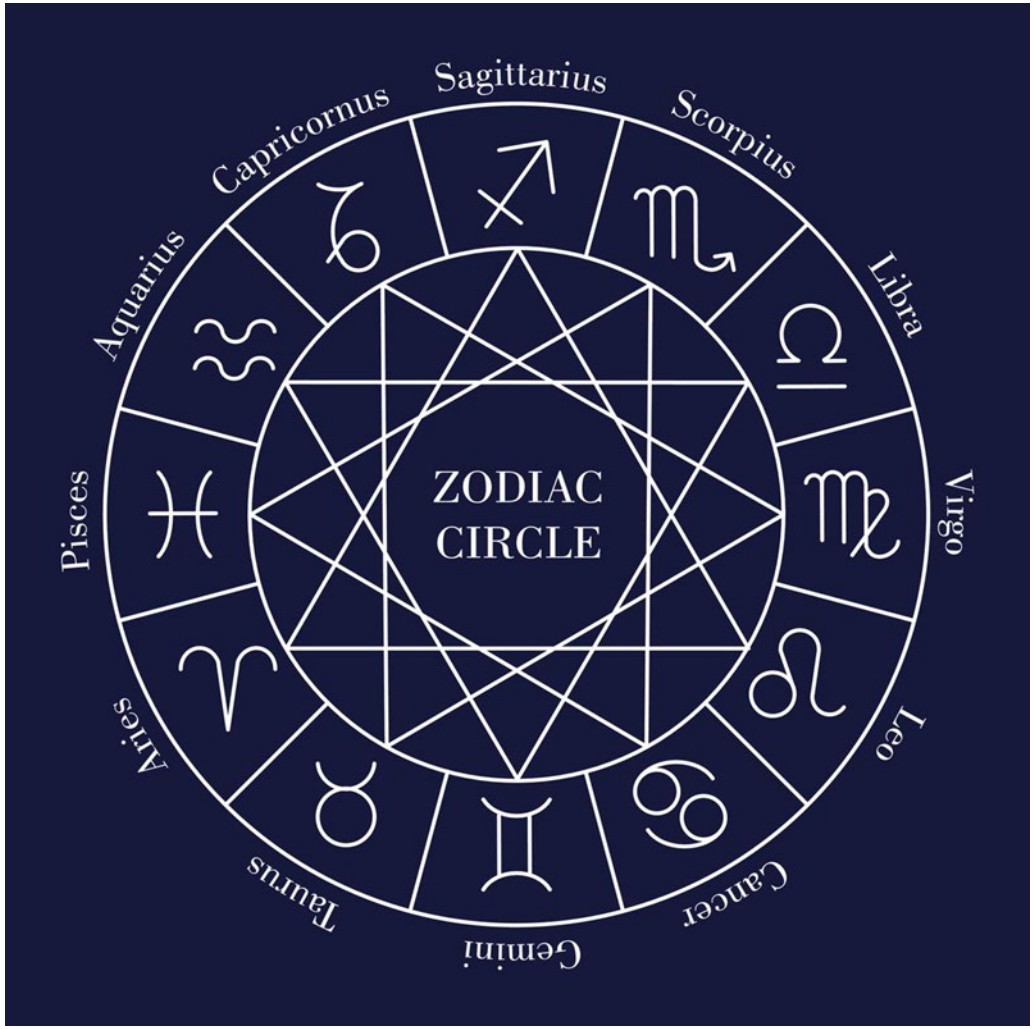
Cold Reading

- Cold Reading is a form of entertainment
- Unfortunately it is also used for fraud:
  - Social engineering
  - Phishing/smishing
  - Phone Scams
- Requires props, acting, rituals, terminology (PART)
- Today's Risk Management Frameworks also use PART

Crystal Balls/Palmistry/Graphology

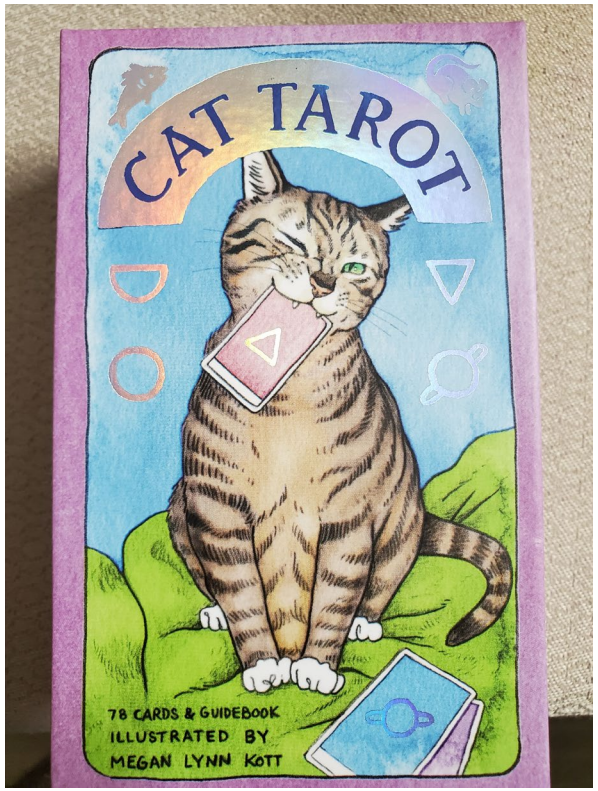


ASTROLOGY

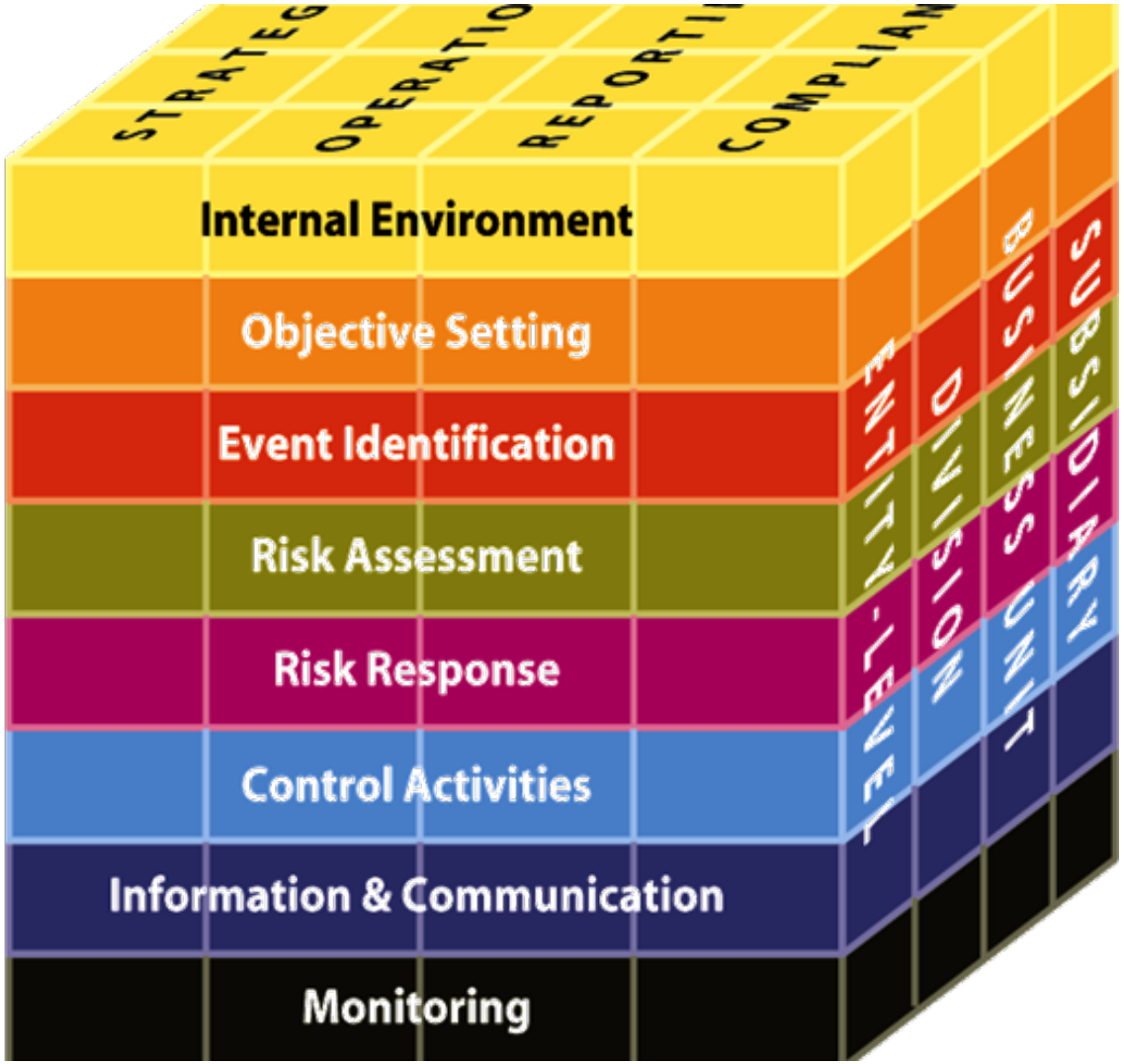


Date	Month	Zodiac Sign	Sign	EFAW
12/21-1/21	January	Capricorn	Goat	Earth
1/22-2/21	Feb	Aquarius	Lovers	Air
2/22-3/21	March	Pisces	Fish	Water
3/22-4/21	April	Aries	Ram	Fire
4/22-5/21	May	Taurus	Bull	Earth
5/22-6/21	June	Gemini	Twins	Air
6/22-7/21	July	Cancer	Crab	Water
7/22-8/21	August	Leo	Lion	Fire
8/22-9/21	Sept	Virgo	7 virgins	Earth
9/22-10/21	Oct	Libra	Scales of Justice	Air
10/22- 11/21	Nov	Scorpio	Scorpion	Water
11/22-12/21	Dec	Sagittarius	Bow and Arrow	Fire

Tarot Cards



PART FOR RISK MANAGEMENT



The 5 Risk Management Components

A beacon of light in uncertain times.™

Coordination of Risk Management

Recognize that not everyone views risk the same way.

Does your organization/department follow an Global Framework (GF) or Functional Framework (FF)?

If Both GF and FF are they the same? Different?

Define and document Risk Capacity, Risk Appetite and Risk Tolerance levels. (Rituals)

Asking questions is the best way to explore more detail.

Risk Management Rituals

Risk Governance:

- Risk Capacity
- Risk Appetite
- Risk Tolerance

Risk Identification: ACTING

- Asset
- Threat
- Vulnerability
- Time/Application

Risk Assessment/Analysis: ACTING

- Possible/Probability Occurrence* Possible/Probability Impact (primary and secondary)
- Risk Ranking

Risk Response: ACTING

- Cost Versus Benefit
- Accept, Avoid, Mitigate, Transfer
- Residual Risk = Inherent Risk minus Control Risk

Monitoring and Reporting: RITUAL/ACTING

- KRIs
- Reporting
- Communications

Terminology: TERMINOLGY

- Risk Asset
- Threat Actor
- Threat Community
- Vulnerability
- Impact

What is Risk? Differences?

ISO 31000, *risk is the "effect of uncertainty on objectives."*
and an *effect* is a positive or negative deviation from what is expected

- Both internal of external
- Goal oriented not event oriented
- Create and protect value

COSO, *risk is* the *possibility that events will occur and affect the achievement of objectives.*

NIST, the extent to which an entity is *threatened by a potential circumstance or event*, and typically a *function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.*

Risk Management 101 – COSO & FAIR

- *Enterprise risk management* as a process, effected by an entity's board of directors, management, and other personnel, applied in strategy-setting and across the enterprise, designed to *identify potential events* that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (COSO)

- The combination of personnel policies, processes, and technologies that enable an organization to cost-effectively *achieve and maintain an acceptable level of loss exposure* (FAIR)

ISO 31000/NIST Definition Risk Management

Risk management refers to a *coordinated set of activities and methods that is used to direct an organization and to control* the many risks that can affect its ability to achieve objectives. (ISO 31000)

- The term *risk management* also refers to the program that is used to manage risk. This program includes risk management principles, a risk management framework, and a risk management process.

The program and supporting processes to manage information security risk to organizational operations. (NIST)

- Including mission, functions, image, reputation, organizational assets, individuals, other organizations, and the nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

TA(M) – Cold Reading

Time – It may have happened to you in the past, or will happen in the future, but it will happen! So please search your memory and let me know which one it is.

Application – It may not have happened to you, it could have happened to someone you know, someone you care about, someone you work with, or a neighbor.

Metaphors – Meaning is different from what I said. When I said that you would be embarking on a journey, it might not be a physical journey but a spiritual or emotional journey.

No matter what the circumstance, the cold reader will subtly shift and move the time, application, or use metaphors to indicate that what they said will happen to you.

Probable versus Possible

Almost anything is possible; we need to focus on probable within a degree of error.

Focus on more probable and/or damaging events first.

High-value assets.

High-frequency threats.

Probable threat communities and threat actors.

Triage methods can help identify.

Who Owns Risk?

Who owns risk?

- Board
- Executive management
- Operational management
- Everyone?

Risk is owned by the person who controls that risk.

That person makes all decisions regarding that risk, especially the response.

Monitors “exception reporting” – work-arounds.

Identifying Risk "Themes"

Risk identification "brainstorming" participants stick to "their" themes.

Risk is *calibrated* against what we know and think we know (read/hear) – environment, organizational structure, processes, controls, or what we currently monitor.

Generally, we should spend more time on risks that we have already experienced.

Cold reading follows themes that apply to the client.

Identifying Possible Risk Themes

BEAR HILL ADVISORY GROUP

Themes of Cold Reading

- Career
- Health
- Relationships
- Money
- Travel
- Education
- Adventure

Themes of Risk Management

- Strategy
- Sales/Customers
- Products/Services
- Costs/Suppliers
- Innovation/Agility
- Information Technology/Data
- Human Resources/Employees
- Finance/Capital
- Geopolitical
- Natural Disaster
- Macroeconomic
- Regulatory/Governmental

RISK IS IN THE EYE OF THE BEHOLDER

Application – Method to calibrate the organization to others (POV)

Identification should first focus on general risk applications

General applications can impact multiple functional risk groups – commonality

- Fraud
- Retaining/attracting quality associates
- Health and safety
- Brand and reputation
- Regulatory

Specific application risks

- IT/data risk
- CIOs see ransomware
- CFOs see business email compromise

CEOs see all the risks that other CEOs have lost their jobs over

Time

Discussion of risk should be anchored in time

Risk that happened in the past

Risk that you believe are current trends

Risk that you will encounter in the future

Speed of the Risk VoR™ impacts risk management

Velocity of Risk (VoR™)

Velocity of risk – The speed of the causation, impact, duration, and normalization of an event on a risk asset

This impact may be positive – upside or opportunity risk – or negative – downside or adverse risk

VoR impacts event onset, duration, recovery, and normalization.

Concept developed by a team lead by Dr. Sridhar Ramamoorti (U. of Dayton)

VoR Practical Application

Most organizations focus on downside risk

Bias towards high-velocity risks versus low-velocity risks

Downside risk + high velocity = Surprise!

Upside risk – value creation; downside risk – value preservation

Low-velocity risks cause disproportionate impact (InfoSec)

Low velocity, upside risks – emerging technology adoption – 5G, blockchain

Granularity of Risk Identification

Most risk identification stops at the “what” and “when.”

A more detailed analysis is required to have an effective risk management program.

Threat community – nation state, organized crime, insider – privileged, non-privileged

Threat profile – motive, primary intent, target characteristics, preferred target, capabilities, concern for collateral damage

Threat capability – skills

Targeted assets

Threat agent risk assessment

ARE THESE RISKS THE SAME?

You're a defense contractor and a nation state targets your company for confidential information. This actor has been known to attack externally using cyber espionage, as well as internally by bribing employees.

You're a defense contractor that practices agile management. People work on teams based on a project basis. During the project, they are afforded privileges to datasets. There is no formal notification to IT when the project has wrapped up. As a result, employees might have access to confidential data.

Primary and Secondary Risk

Probability/Possibility of Primary Risks

- Example of Primary Risks:
  - Data Breach
  - Ransomware
  - BEC

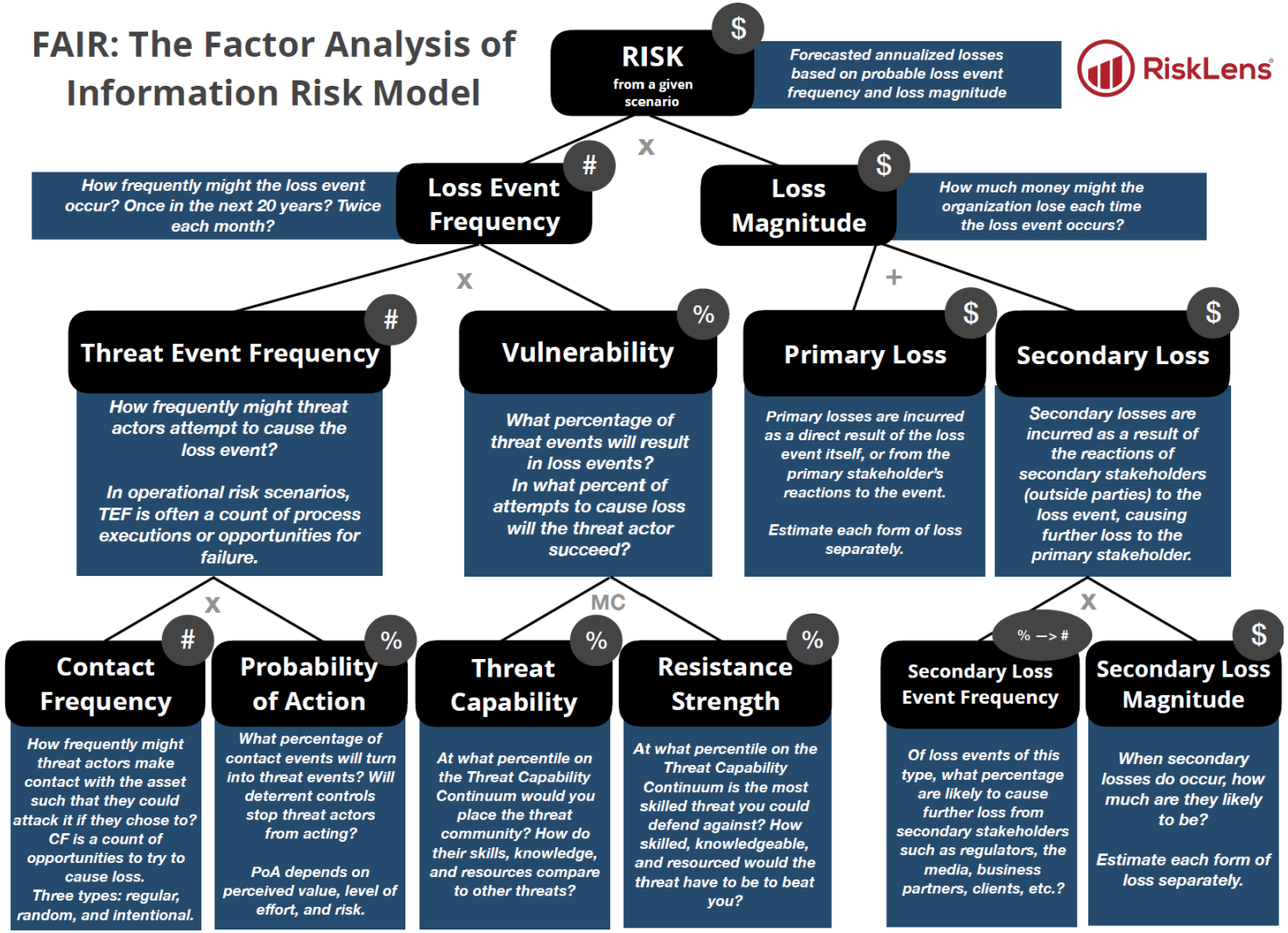
Probability Binomial Secondary Risks

- Example of Secondary Risks:
  - Forensic Experts
  - Credit Monitoring
  - Legal Fees
  - Regulatory Fines

FAIR Model

- Fundamental Analysis of Information Risk- FAIR Institute
- Ontology provides for quantification of Risk
- Each Risk is broken down to primary and secondary events
- Each event has a probability and a magnitude

FAIR MODEL EXPANDED



SUMMARY

Risk Management should be *grounded in reality and facts*, not possibilities and potential.

Focus on most *probable risk causing the greatest impact* first.

Understand and *focus on the time frame of risk.*

Velocity of risk is much more than "response/mitigation."

Understand and *study risk granularly by asset, threat community, threat actor, and vulnerability.*

Look at *primary and secondary impacts* and probability differently.

VIRTUAL READING

Meant to be fun.

What I say, may or may not have meaning to you, only you can tell.

Don’t worry if you don’t understand some of my references now; they may make sense to you in the future.

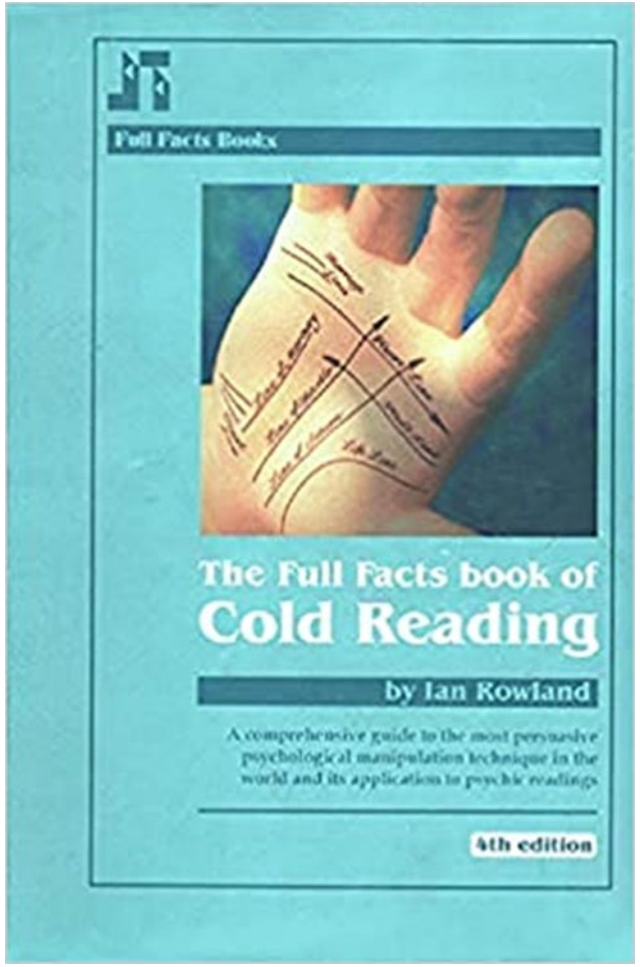
Nothing of this is meant to be too personal. I can’t help where the cards take me, so if I get personal, don’t feel like you must answer.

Learn More About Cold Reading

Ian Rowland Author

A comprehensive guide to the most persuasive psychological manipulation technique in the world and its application to psychic readings. Cold reading can loosely be described as “how to talk to a complete stranger as if you have known them all your life.” This definitive yet easy-to-read guide explains every aspect of cold reading in detail. Although the book focuses on how cold reading is used within the psychic industry, many cold reading principles have applications in other fields such as selling, negotiation, management, and therapy. This is a “must read” book for anyone interested in the psychology of persuasion.

Ianrowland.com



Questions and Contact Information

Jack P. Healey CFE, CPA/CFF, CRISC

CEO

Bear Hill Advisory Group

770.362.2008

JHEALEY@BHAGRP.COM

@CyberBizRescue

@BHAGRP

www.bhagrp.com

GEEK WEEK
ISACA Atlanta

A beacon of light in uncertain times.™