A beacon of light in uncertain times.™

Risk Management – Deep Thoughts and Better Results

Presentation for the Kennesaw State University

March 31, 2021

Jack Healey CFE, CFF, CPA, CRISC

CEO Bear Hill Advisory Group

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, RMS 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.

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

Improve your Risk Identification

Purpose of today's discussion is to view your risk management differently.

Help you become better at identifying risk.

Learn about power of probability, value of time, risk application.

What is the Velocity of Risk?

What is Risk Identification Granularity?

Primary risk and probability of secondary risk?

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

Risk Management 101

Risk Governance
- Risk Capacity
- Risk Appetite
- Risk Tolerance

Risk Identification-
- Asset
- Threat
- Vulnerability

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

Risk Response
- Cost v Benefit
- Accept, Avoid, Mitigate, Transfer
- Residual Risk = Inherent Risk-Control Risk

Monitoring and Reporting
- KRI's
- Reporting
- Communications

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

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

Speak the same Language

Recognize not everyone views risk the same way.

Understand what ORM or ERM the team uses.

“Level Set’ the definitions prior to the discussion.

Document Risk Appetite and Tolerance.

Asking questions is the best way to explore more detail.

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

What is Risk?

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.*

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

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)

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

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.

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

Risk Management and the Time Variable

Our time and resources are limited.

Identification approach needs to be disciplined.

Probable/Possible Primary and Probable Secondary Risks.

Possibilities are endless.

What's in your future.

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

Identifying Risk Themes (Application)

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 which we have already experienced.

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

Time and Application

Time- what is the time period that your risk identification is covering?

- Risk which happened in the past
- Risk that you believe our current trends
- Risk that you will encounter in the furture

Application- Method to calibrate the organization to others.

- CIO's see ransomware as a risk
- CFO's see Business Email Compromise
- CEO see all risks that other CEO's have lost their jobs over

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

Identifying Functional Risk

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

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

EXAMPLES HOW APPLICATION IMPACTS IDENTIFICATION

Theme: Natural Disasters

- Frequency
- Impact
- Risk Response

Theme: Ransomware

- Frequency
- Impact
- Risk Response

Always include risk events which have occurred in the past as probable events for the future. Our past gives us a hint as to our future

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

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.

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

VoR Practical Application

Most organizations focus on downside risk.

Bias towards High Velocity Risks vs Low Velocity Risks.

Downside Risk + High Velocity = Surprise!

Upside Risk- Value Creation; Downside Risk- Value Preservation.

Low Velocity Risks cause disproportionate impact (Info Sec).

Low Velocity, upside risks- Emerging Technology Adoption- 5G, Block Chain.

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

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.

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

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's basis. During the project hey are afforded privileges to data sets. There is no formal notification to IT when the project has wrapped up. As a result, employees may have access to confidential data.

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

Primary and Secondary Risk

Probability / Possibility of Primary Risk

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

Probability Binomial Secondary Risks

- Example of Secondary Risks
  - Forensic experts
  - Credit monitoring
  - Legal fees
  - Regulatory fines

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

SUMMARY

Speak the same language.

Understand Time, Risk Application.

Velocity of Risk is much more than ‘response/mitigation’.

Look at risk granularly by Asset, Threat Community, Threat Actor, Vulnerability.

Look at primary and secondary impacts and probability differently.

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

Questions and Contact Information

Jack P. Healey CPA, CFF, CFE, CRISC

CEO

Bear Hill Advisory Group

770.362.2008

JHEALEY@BHAGRP.COM

@CyberBizRescue

@BHAGRP

www.bhagrp.com

© 2021 BEAR HILL ADVISORY GROUP LLC. ALL RIGHTS RESERVED.

A beacon of light in uncertain times.™