Beware of Whispers in the Night: Why Risk Assessments Provide Limited Value

Geary W. Sikich
Logical Management Systems, Corp.

One of the most interesting and overlooked aspects of risk management is what I refer to as risk entanglement. If you identify (observe) a risk, someone – even one, many miles away – identifying the same risk; both take action to mitigate the risk. This instantly changes the risk's properties for both, creating a need to constantly consider risk mitigation actions. This works both ways, depending on who acted first. And we do not even have to be in communication with each other. Risk is not static. Risk changes by each action taken to mitigate or leverage it. Now, multiply "risk entanglement" by all the identifiers of that risk and all the actions taken to mitigate this ever-changing risk (each action taken to buffer against risk realization changes the nature of the risk) and you get a potentially chaotic cascade effect. How is it that the world remains relatively stable when so much risk is constantly mutating due to mitigation? It's relatively simple, our risk management activities are short lived and generally have been limited to certain types of risk management response. This needs to change in order to bring risk management to the forefront of executive management thought as they develop and execute strategy, goals and objectives.

Keywords: risk management, risk entanglement, consequences, risk mitigation, business continuity, contingency, recovery time objective, recovery point objective, maximum tolerable outage, risk appetite, risk tolerance, risk saturation, risk absorption, business impact assessment/analysis, risk mosaic, risk cross over, asymmetry

INTRODUCTION

I just finished reading two very different books; one a novel, the other a fact-based investigative report. The first book, entitled "Second Sleep" by Robert Harris (ISBN 9780525656692) is fiction. The second book, entitled "Lights Out" by Ted Koppel (ISBN 9780553419962) is a critical look at how unprepared we are for a cyberattack on our electric grid. Two very different books, yet they overlap in many ways.

The setting in Harris' book is post-apocalyptic. Koppel's book focuses on our lack of preparation and our vulnerabilities in the interconnected world that we live in. In Harris' book the main character comes upon books, letters and objects that are now considered heretical. He reads a letter, dated 22 March 2022 that outlines six scenarios; excerpted below:

> **"We have broadly identified six possible catastrophic scenarios the fundamentally threaten the existence of our advanced science-based way of life:**

1. **Climate change**
2. **A nuclear exchange**
3. **A super-volcano eruption, leading to rapidly accelerated climate change**
4. **An asteroid strike, also causing accelerated climate change**
5. **A general failure of computer technology due either to cyber warfare, an uncontrollable virus, or solar activity**
6. **A pandemic resistant to antibiotics**

Our purpose is not to propose counter-measures to avert any of these potential catastrophes – a task that, in the cases of 3 and 4, is in any case impossible – but to devise strategies for the days, weeks, months, and years following such a disaster, with the aim of the earliest possible restoration of technical civilization."

In Koppel's book (page 19) a quote from Jon Wellinghoff (who was chairman of the Federal Energy Regulatory Commission (FERC)) cites an analysis by FERC concluding:

"that if nine of the country's most critical substations were knocked out at the same time, it could cause a blackout encompassing most of the United States"

Are the six scenarios somewhat familiar from a risk management/business continuity planning perspective? They should be. If I recall, I have touched on many of these in other articles and in consulting engagements. But, hey, Harris' book is a novel, right?

As regards Koppel's book, there are many naysayers that have voiced the impossibility of bringing the national grid system down due to its resilience. Yet, we have experienced blackouts, brownouts and disruption due to natural disasters and human error. We are now seeing that utilities are incorporating mandatory termination of electric supply due to lessons learned from the devastation of California's recent wildfires.

Today we are seeing Australia battle against wildfires that have literally burned some towns down to the ground.

Climate change has begun to alter how we look at the weather. As I write this on 3 January 2020; I recall recent days being able to sit outside in near 60-degree Fahrenheit, enjoying a good book. I live just outside of Chicago.

Steve Jurvetson, venture capitalist and founder of Future Ventures posted the following on Flickr:

1/4 of us now think Apollo was Fake News?!?
Why, oh why, are we regressing in critical thinking?
"Members of Gen X and Millennials believe in growing numbers that the moon landings were faked, from 4% fifty years ago, as the landings were actually occurring, to as high as 25% in some recent surveys."
— *adAstra* Apollo 11 50th Anniversary Edition 2019
P.S. from a survey of American adults 15 years ago:

- **33% believe in communication with the dead**
- **39% believe astrology is scientific**
- **46% deny that human beings evolved**
- **49% don't know that it takes a year for the Earth to orbit the sun**
- **67% don't know what a molecule is**

— from Posner's *Catastophe* book that we used in a class I co-taught at Stanford Law School, 2004 blog
http://jurvetson.blogspot.com/2004/10/spooks-and-goblins.html

As tensions flare in Iraq and Iran in the aftermath of the US bombing that killed Qassem Soleimani, Iran's Quds Force commander, the threat of retaliation and counter-retaliation simmer.

Kim Jong Un just announced that North Korea is considering the restart of long-range ballistic missile testing.

All this and we are not even through the first week of 2020! (Coronavirus was not an issue at this time – just wait a couple of weeks though).

Unseen Consequences are Harmless Until They Are Not

Due to the non-static nature of risk, exposures constantly change. Mitigation has the effect of altering the risk so that a new exposure is created. Mitigation buffers risk temporarily. One thing that is not taken into account when doing a risk assessment is the action of others who have the same risk exposure and are taking mitigation actions to buffer the risk exposure that they have. It is imperative to develop a mindset of constant risk monitoring and buffering activities. See my article on thinking like a commodities trader when it comes to risk.

Unpredictability is the new norm today. The breadth of unseen consequences poses a risk to government and business alike. "Because we are asking the wrong questions precisely, we are getting the wrong answers precisely; and as a result, we are creating false positives." Unless we change this paradigm, we will continue to get false positives and find ourselves reacting to the unseen consequences of events instead of being proactive.

Effective risk management can only be achieved when one understands the breadth of an enterprise's sphere of operations. Internal programs must integrate with external exposures. The enterprise cannot effectively implement a risk management program if it does not include its "value chain" in the process. The problem faced by today's enterprise is: "how to effectively design and implement a broad-based risk management program."

Creating a Risk Mosaic Requires Constant Updating. Consequence Identification and Control: Identification and quantification of potentially disruptive events that could escalate into a crisis must be accomplished so that controls and safeguards can be developed to prevent or minimize the impact of any type of disruption. When the right precautionary approach is to consider the unseen as potentially harmful; how do we operate?

The reality of risk today - Volatility, uncertainty, complexity and ambiguity parameters are broader with more prevalent swings. Have you adjusted your competitive strategy thinking and models?

Is Business Continuity Planning Dying, Dead or Just Discounted?

What do we really know about business continuity? In the view of Senior Management, every day that the organization stays in business equals continuity. Does anyone then, really care about business continuity planning? If a constant tactical approach to business continuity planning is taken by business continuity planners will Senior Management ever respect the value of the product that is produced? Do business continuity planners actually add value or are they distracted in their planning perspectives?

How many business continuity plans have a "trade war" appendix? How many business continuity planners seek to understand sovereign debt, supply chain points of failure, logistics of recovery and the organization's strategic initiatives? And, that is just to name a few of the issues that need to be analyzed, studied and have valid contingency action plans in place for.

Scare Tactics or When Disaster Strikes, is it Game Over?

An often-cited quote used by many:

> ***"After a major disaster, more than 40% of businesses are dead in the water, according to the Federal Emergency Management Agency. They never reopen their doors. And among those that do stay open, their survival is only temporary: roughly 70% of them close within two years.***

This is why every business needs to take disaster planning seriously. Without a plan in place for preventing a disaster, or responding to it, your organization will become just another statistic."

Really? Does the above ring true? Actually, most business startups don't last a year – read that as a high rate of failure associated with opening a business; not because of a disaster, because of competition, poor execution of the business plan, underfunding, etc. By the way a colleague of mine decided to check the statistics cited above and it seems that the percentage is a bit of a myth that has been fostered throughout the years. We first heard this percentage in the late 1980's; almost 40 years ago.

In a recent survey, BC Management asked respondents to choose their top 5 to 10 Event Categories. The categories and sub-categories

Accident
- **Chemical spill**
- **Collision**
- **Contamination**
- **Explosion**
- **Fire**
- **Nuclear contamination**
- **Power outage**
- **Spillage/ Leakage**
- **Structural failure**
- **Water (main break/ loss/ failure)**

Human/ Business Disaster
- **Bomb threat**
- **Brand/ Social media damage**
- **Civilian unrest/ Political instability**
- **Class action lawsuit**
- **Corporate fraud**
- **Disgruntled employee**
- **Embezzlement**
- **Espionage**
- **Extortion**
- **Financial market disruption**
- **Government shutdown**
- **Health/ Safety issue**
- **Loss of key executives - Death, Kidnapping or assassination**
- **Negligence**
- **Pandemic/ Disease**
- **Protest**
- **Robbery/ Theft**
- **Sabotage**
- **Strike**
- **Supply chain disruption**
- **Terrorist activities**
- **Vandalism**
- **War or insurrection**
- **Workplace violence**
- **World events - conventions, sports, etc.**

Natural
- **Dust storm**
- **Earthquake**
- **Fire/ Wild fires**
- **Flood**
- **Heat - excessive**
- **Hurricane**
- **Ice storm/ Winter weather**
- **Landslide**
- **Tornado**
- **Tsunami**
- **Typhoon**
- **Volcanic eruption/ Ash cloud**

Technical
- **Change management**
- **Computer virus**
- **Cyberspace attack**
- **Data breach**
- **Hardware issues**
- **Network/ Communication (Outage)**
- **Scheduled testing**
- **Server issues**
- **Software issues**
- **Technology migration**

Note: the survey did cite "**Loss of key executives - Death, kidnapping or assassination**" although I am not sure if this would relate to recent events (i.e., Qassem Solimani, Iran's Qud Commander)

In the long run, just think of all the companies that have survived and thrived after disasters – Exxon – The Valdez, BP – Deepwater Horizon, Union Carbide – Bhopol, Facebook, Microsoft, Apple, Firestone, Ford, General Motors, AIG, Bank of America and a host of other companies have paid huge fines, experienced disasters, etc. and they still are around today and doing well. Boeing – 737, an ongoing

debacle and Boeing is still making airplanes (albeit not 737's at present) and we are still boarding them. So, while we are angry, concerned and afraid with the latest data breach revelation concerning Equifax, when it comes down to it, we quickly forget and move on. Capital One is the latest to reveal a data breach exceeding 100 million, so what's new?

Wandering in a Hall of Mirrors

Every day that a business stays in business is success for senior management. It means that continuity of operations has been achieved, for that day. It is the barometer for future business decisions. Ask yourself, "How many business executives adhere to the business continuity plan?" Do a survey and find out. Find out if they actually know what is in the plan. Find out what they think of the planning process and the terms that we embed in our documents – **RTO** (Recovery Time Objective), **RPO** (Recovery Point Objective), **MTO** (Maximum Tolerable Outage), **Hot Site**, **ICS** (Incident Command System), **NIMS** (National Incident Management System), **Risk Appetite**, **BIA** (Business Impact Assessment/Analysis), the list goes on and on.

What does the decision maker care about? They care about meeting the goals and objectives set out in the strategic plan; beating the competition, staying competitive, reducing costs and increasing shareholder value. How this gets accomplished is middle management's focus and there is a lot of pressure to make it happen every day.

As business continuity planners are you assisting or obstructing the accomplishment of the above cited areas of concern that senior management and middle management are focused on? Sure, you can tell them how many work stations, computers, printers, copiers, applications, etc. that the BIA report contains. But, so what? Much of the information is readily available from the purchasing department and facilities management. So, where is the value proposition for business continuity planning? Are we practicing a dying, dead or discounted arcane, legacy function, because that's the way it's always been done?

Senior management will take whatever risks they deem necessary in order to secure the goals and objectives for the organization (including their performance bonus, salary package, etc.). You can read that as a "healthy or hearty risk appetite". Where does business continuity planning fit in the mix of things that are on the plate of senior management? Survey's give lip service to the importance of resilience for the organization; same with Corporate Social Responsibility (CSR), climate change, etc. However, does change really occur due to concern or is it as a result of being able to cut costs and make more profit?

The "Asymmetric Bet"

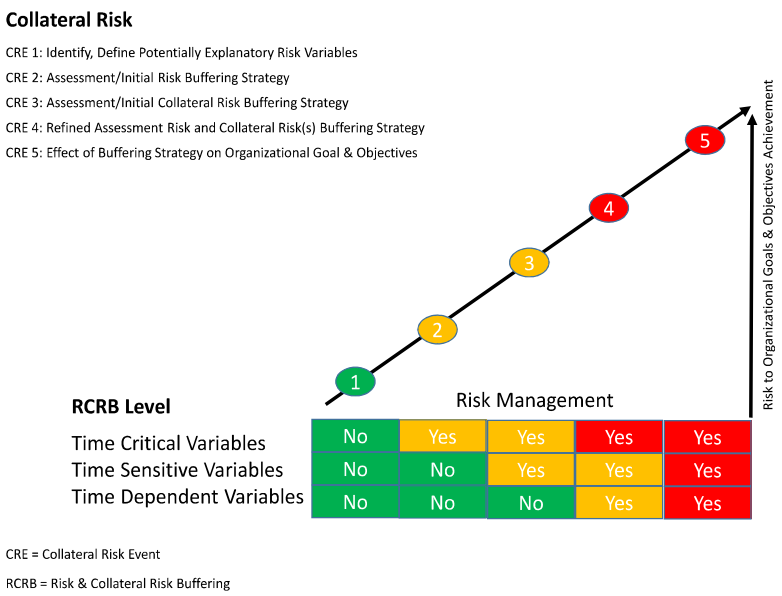
Risk is asymmetric; that is, it is not identical to every individual assessing the risk that has been identified. Some see the risk as an operational issue, others may see it as a financial issue, still others may see it in terms of insurance coverage, etc. We need to understand where the cross over points are when implementing risk mitigation measures. Risk cross over is the point at which the cost to mitigate (protect against risk realization) becomes greater than the asset exposed to risk realization.

In his 1921 classic, *Risk, Uncertainty, and Profit*, Frank Knight states the following:

> "There are other ambiguities in the term "risk" as well, which will be pointed out; but this is the most important. It will appear that a measurable uncertainty, or "risk" proper, as we shall use the term, is so far different from an unmeasurable one that it is not in effect an uncertainty at all. We shall accordingly restrict the term "uncertainty" to cases of the non-quantitative type. It is this "true" uncertainty, and not risk, as has been argued, which forms the basis of a valid theory of profit and accounts for the divergence between actual and theoretical competition."

The following graphic, Figure 1: Collateral Risk Matrix, depicts collateral risk a reflection of "true" uncertainty.

FIGURE 1
COLLATERAL RISK MATRIX



CONCLUSION

In order for any organization to succeed in today's fast paced, globally interlinked business environment the ability to identify and assess risk and to identify collateral risk needs to be addressed. When you take Management (leadership & decision-making), Planning, Operations, Logistics, Communications, Finance, Administration, Infrastructure (Internal & External), Reputation, External Relations and other dependency issues into account, there is potential for significant impact on six areas that I consider critical for organizations:

1. Strategy (Goals & Objectives)
2. Concept of Operations (How goal and objective are achieved)
3. Organizational Structure (How does the organization actually work)
4. Resource Management (Human, Financial, Physical, Data)
5. Core Competencies (Essential skills)
6. Pragmatic Leadership (at all levels with a common understanding of terminology)

We live in a world full of consequences. Our decisions need to be made with the most information available with the recognition that all decisions carry with them flaws due to our inability know everything. Our focus should be on how our flawed decisions establish a context for flawed Risk Threat Hazard Vulnerability (RTHV) assessments, leading to flawed plans, resulting in flawed abilities to execute effectively. If we change our thought processes from chasing symptoms and ignoring consequences to recognizing the limitations of decision making under uncertainty, we may find that the decisions we are making have more upside than downside.

It's all about targeted flexibility, the art of being prepared, rather than preparing for specific events. Being able to respond rather than being able to forecast, facilitates early warning and proactive response to shifts in your market segment.

REFERENCES

Apgar, D. (2006). *Risk Intelligence – Learning to Manage What We Don't Know*. Harvard Business School Press.

BC Management Annual Survey. (2019). Retrieved from https://www.bcmanagement.com/

Davis, S.M., & Meyer, C. (1998). *Blur: The Speed of Change in the Connected Economy*.

Frank, H. (2015). *Knight, Risk, Uncertainty, and Profit*. Boston MA: Hart, Schaffner and Marx; Houghton Mifflin, 1921. Retrieved from http://oll.libertyfund.org/titles/306

Harris, R. (2019). *Second Sleep*. ISBN 9780525656692

Jurvetson, S. (2004). *Spooks and Goblins*. Retrieved from http://jurvetson.blogspot.com/2004/10/spooks-and-goblins.html

Jurvetson, S. (2019). *1/4 of us now think Apollo was Fake News?!?* Retrieved from https://www.flickr.com/photos/jurvetson/48717810172/in/photostream/

Kami, M.J. (1988). *Trigger Points: how to make decisions three times faster*. McGraw-Hill. ISBN 0-07-033219-3

Klein, G. (1998). *Sources of Power: How People Make Decisions*. MIT Press. ISBN 13 978-0-262-11227-7

Koppel, E. (2015). *Lights Out*. ISBN 9780553419962

Levene, L. (2003, April 8). *Changing Risk Environment for Global Business*. Union League Club of Chicago.

Orlov, D. (2008, June 1). *Reinventing Collapse* (First Printing edition). New Society Publishers. ISBN-10: 0865716064, ISBN-13: 978-0865716063

Rock, T. (2018, March 27). *The truth about what business continuity looks like today*. Invenio IT.

Sikich, G.W. (1993). *It Can't Happen Here: All Hazards Crisis Management Planning*. PennWell Publishing.

Sikich, G.W. (1995). *The Emergency Management Planning Handbook*. McGraw Hill.

Sikich, G.W. (2002). *Graceful Degradation and Agile Restoration Synopsis*. Disaster Resource Guide.

Sikich, G.W. (2002, May). *Aftermath September 11th, Can Your Organization Afford to Wait*. New York State Bar Association, Federal and Commercial Litigation, Spring Conference.

Sikich, G.W. (2002, Winter). September 11 Aftermath: Ten Things Your Organization Can Do Now. *John Liner Review*, *15*(4).

Sikich, G.W. (2003). *Integrated Business Continuity: Maintaining Resilience in Times of Uncertainty*. PennWell Publishing.

Sikich, G.W., & Stagl, J.M. (2005). *The Economic Consequences of a Pandemic*. Discover Financial Services Business Continuity Summit.

Tainter, J. (1990, March 30). *The Collapse of Complex Societies*. Cambridge University Press. ISBN-10: 052138673X, ISBN-13: 978-0521386739

Taleb, N.N. (2007). *The Black Swan: The Impact of the Highly Improbable*. Random House. ISBN 978-1-4000-6351-2

Taleb, N.N. (2008, October 14). *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets* (Updated edition)0 Random House. ISBN-13: 978-1400067930

Taleb, N.N. (2009, October 18). *Common Errors in Interpreting the Ideas of The Black Swan and Associated Papers*. NYU Poly Institute.

Taleb, N.N. (2010). *The Black Swan: The Impact of the Highly Improbable* (Second Edition). Random House. ISBN 978-0-8129-7381-5

Vail, J. (2006). *The Logic of Collapse*. Retrieved from www.karavans.com/collapse2.html