Developing a Framework and Methodology for Assessing Cyber Risk for Business Leaders

Howard Miller
LBW Insurance and Financial Services

Charla Griffy-Brown
Pepperdine University

Cyber Risk is in fact an existential threat to modern business. In order to effectively deal with cyber risk it must be explained in terms of overall risk theory and frameworks enabling better decisions regarding cyber risk. This paper develops a more effective and unified approach to risk enabling better cyber risk decisions. It provides an overview of the concepts and theories of risk that prevail as well as a framework for decision making that can be applied to cyber risk. This framework is unique in that it provides practical tools for decision-making and a conceptual model tying cyber risk to broader risk. Based on this framework, a database tool was applied and tested across 20 industry verticals.

INTRODUCTION

Risks are an integral part of modern society and can be found everywhere: in our homes, politics, economic systems, lifestyles, finances, and even in our environment. Risk taking is also inherent in business driving innovation, development and wealth creation. Importantly, digital architecture and agile data structures permeate all elements of modern society including those just mentioned. In business, the necessity of identifying and dealing with cyber risk is paramount. Cyber Risk is in fact an existential threat to modern business as evidenced by the businesses which have had to declare bankruptcy following a breach. However, in order to effectively deal with cyber risk it must be explained in terms of overall risk theory and frameworks enabling better decisions regarding cyber risk. Is there a more effective and unified way to consider risk that will help decision-makers deal more effectively with cyber risk?

This paper aims to answer this question and provide an overview of the concepts and theories of risk that prevail as well as a framework for decision making that can be applied to cyber risk. This framework is unique in that it provides practical tools for decision-making and a conceptual model tying cyber risk to broader risk. As a first step, a summary is given of the attempts at construing the concept of risk. Previous studies demonstrate that our relationship to risk is influenced by a number of factors and in order to deal effectively with cyber risk we must re-conceptualize risk overall. Following this, our methodological approach for testing the theory will be explained. The final sections will include a detailed description of the resulting framework followed by a conclusion. These trends raise significant questions that business leaders and decision-makers need to consider: What are these business models? Are there trends and themes? Based on a clearer understanding of the evolution of cybercriminal activity organizations can begin to develop more sophisticated approaches to calculate appropriate risk in business

initiatives and develop models for addressing an attack. This analysis will identify developing business models and their revenue streams. These models will then be analyzed using a business model framework to reveal broader themes and if they are sophisticated enough to truly be evaluated as a legitimate business model. We will also consider their impact on risk and mitigation. Based on this evaluation, we will present a risk-based approach for securing an environment without a perimeter against increasingly organized criminals.

THEORY AND OVERVIEW

Risk is inherent in the nature of human existence. Risk knows no boundaries other than an environment absent of risk. As the nature of any successful organization rests upon revenue (operating budget) whether for profit, non-profit, governmental or municipality, there must be a balance between the drive for revenue/operations and an understanding that risk can destroy all future objectives.

Risk in modern times builds on existing foundations of risk, indeed "The concept of risk is as old as mankind" (Garaczi 2013, p. 1). However, the role of risk became significantly more prominent in the late 20th and early 21st centuries. Bernstein (1998) even suggests that the mastery of risk defines the boundary between modern times and the past. This may seem contradictory when you consider that the further we look back in time, the greater the exposure of (pre)modern societies to hazards (Dessewffy 2002). The seeming contradiction can be resolved by creating a distinction between the concepts of risk and hazard, as described in detail in later sections of this paper. Providing the foundations for modernization, scientific and technological development eliminated the hazards and risks posed by nature, while giving rise to new ones (Lányi 2011). Obviously, the level of development in this regard varies by culture and society. The lower the level of modernization in a society, the more risks and hazards are presented by nature. That is, societies increasingly face technological risks as they develop; however, as a result of globalization, the risks of more developed societies may also impact other (possibly less developed) societies: in the course of human history, personal risks have evolved into global ones. Ulrich Beck captures this argument by saying that "the social production of wealth is systematically accompanied by the social production of risks" (Beck 1986/2003, p. 25).

As a result, the problems of resource distribution are outweighed by the risks stemming from the production, identification and distribution of risks produced by means of science and technology. He calls this risk society, which replaces industrial society when the hazards created by social decisions go beyond the boundaries of insurability (Beck 1986/2003), i.e. protection is no longer provided by private insurers. Consequently, Beck maintains that private insurers keep the gates of risk society which is by additional scholarship (Park, et.al., 2012; Teng, et. al., 2012). This is confirmed by recent disasters caused by technology. Park et. al. (2012) inferred both theoretically and empirically that absolute security is non-existent in the field of high-risk technologies; as such technologies no longer involve linear processes, complex interactions will inevitably lead to systemic accidents which is further explored an questioned by Frick (2012) and even further back by Kaplin (1981). Furthermore, systemic accidents cannot be prevented through an ever growing number of security measures, because they merely add to the complexity of systems (Cox, 2008; Alberts, 2011; Teng., et. al., 2013). Beck further argues that tragedies are also attributable to the fragmentation of liabilities, because in the context of global risks, it is mostly impossible to establish personal liability (Vasvari, 2015). Evolving during the development of capitalism, the institution of limited liability may also encourage disproportionate risk-taking, which in turn may be intensified by the softened budgetary constraints of enterprises (Kornai, 2014).

As society has modernized and evolved our ability to transact and operate has been interwoven into the digital architecture and agile data structures that have replaced the analog nature of our past. This digital evolution is tied to the binary as the foundational instructions of digital infrastructure is software code. Software code and digital information itself is at its essence constructed from 0 and 1; a quintessential representation of binary nature of human existence.

From a risk perspective, what has changed is an expansion in scope that now must include both cyber and physical risk. The physical hazards of the past have never disappeared, and their impact is even more

noticeable depending on your location in the world at any given time. Impacts from human kind: ex. Global warming, chemical/nuclear (IE. Fukashima power plant disaster) can compound natural phenomena with technological advancement resulting in an exponential increase in risk (Chiles, 2002). Software code is constantly evolving and a permanent solution to eliminate all bugs, exploits and vulnerabilities is not apparent. As our society can no longer fall back on a paper or analog environment, we must address the cyber risks of our future in addition to our traditional understanding of risk.

What is proposed is a reevaluation of risk management as a process of protecting organizational assets arising out of societal evolution and modernization (Griffy-Brown, et. al., 2016). The goal is to better equip and educate business leaders with a holistic framework to understand risk and through a partnership including government and industry, create a sustainable operational environment. Analysis has been done in discrete areas such as cybersecurity from a technology perspective or even engineering and the connection between physical and security risk (Linkov, et. al., 2013; DiMase, et. al., 2015; Collier, et. al., 2014; Olzak, 2013). We suggest that a more comprehensive risk-based approach is required to address the challenges leaders face in the modern business world. This will allow innovation, increased revenue, reduced costs, and new opportunities for our connected future.

Risk can be measured in terms of volatility. A good place to start is the node. Using a standing wave, the point at which amplitude is at its minimum. This might be considered the beginning and end of all risk. From a representational standpoint 0 risk would be a pre-operational, pre-existing status of an organization. As amplitude increases, boundaries stretch and break. As boundaries stretch and break damage occurs. This is true for all cyber and physical constructs and is the nature of risk itself.

There are many stories of unconscious behavior by individuals or entities that ends in damage due to unforeseen risk. (America's funniest home videos, YouTube, the news). Some minor and comical and some extremely devastating to both organizations and our society. Although risk management can be instinctual the complexity and severity of unknown events requires a conscious and systematic approach. This is the reason that almost all larger organizations employ risk officers and/or risk committees. Regardless of an organization's resources there is no escape from the impact of risk and thus business leaders from all spectrums of wealth and influence can benefit from risk management. Refinement of risk management as a process and the key components used in achieving conscious results will be explained further in the proposed framework.

METHODOLOGY

In order to test the risk framework a database tool was developed based on the framework and applied to - Professional Services: IT Services, Information Security Consulting, Software Development, Various Consulting, Legal Services, Security, Manufacturing: Consumer Goods, Technology, Cosmetics, Distribution, Construction, Insurance Claims Management, Entertainment: Production, Event Services, Post-Production, Show Control Systems. Food Service, Real Estate, Retail, and Non-profits. - actual cases of risk. This applied approach for testing the framework was based on grounded theory methodology. Ethnography involves researchers using direct observation to study participants in their "real life" environment, sometimes over extended periods. Grounded theory (2008) and its later modified versions (e.g., Strauss and Corbin, 1998) uses face-to-face interviews and interactions such as focus groups or work directly with individuals within an organization to explore a particular research phenomenon. Grounded theory was used to help in clarifying less-well-understood problems, situations, or contexts as data was collected across 100 individuals across 20 verticals .

This study used Grounded Theory and to some extent ethnographic methodology to observe and then explore the deployment of this framework in different organizational contexts: non-profit and enterprises of varying sizes and across different industry verticals. This enabled the observations to be developed regarding the use and limitations of this framework.

PROPOSED FRAMEWORK

The proposed framework is broken into three steps. Frameworks with 5 or 6 steps are not uncommon, but to refine and simplify understanding the entire process can effectively fit into three steps. 1. Identify and Analyze, 2. Risk Control and Risk Finance, 3. Administration: Implement and Monitor. Appendix 1 provides specific definitions.

The first step is the most important as you cannot treat a risk that you cannot identify. Thus, a logical approach from the classification of exposers to analysis is contained in step one. Step 2 contains the techniques to control risk and risk finance. Risk finance includes the domain of insurance. Although risk controls and insurance can be implemented without identifying risk exposures they will invariably lead to wasted resources and uncovered losses as these priorities were never identified in step one. Step 3. No organization can benefit without implementing the correct plans and programs. Negligence is possible for educated organizations that knew and had plans to implement effective risk controls and/or insurance and failed to do so.

The goal is to allow leaders to identify and prioritize risk, so resources can be efficiently distributed to meet organizational objectives. Risk tolerance and resource allocation are the responsibility of each organization so the use of internal and external expertise can be critical in making wise decisions. The most effective risk controls and insurance can then be tailored to protect the organization. Projects gain a high likelihood of success with the board and executive support because the priorities are clear.

Through further refinement the entire process can be contained in two key objectives. 1. Prioritize risk. 2. Protect the organization (Figure 1). This cycle remains relevant throughout the existence of the organization. Risk exists in an environment of constant change. What is of greatest concern today may or may not be of the same relevance in the future. Periodic and/or triggered reviews is the only way to adapt to a changing environment. Ability to adapt to change directly correlates with an organization's ability to survive.

FIGURE 1
TWO OBJECTIVES IN THE CONTEXT OF A HOLISTIC RISK MANAGEMENT FRAMEWORK

Each of these two key objectives can be accomplished through a four-step process illustrated below. Integral to this proposed framework is a hierarchy. The objective of this was to utilize the framework as a basis of discussion and communication at various degrees of depth. This way the framework can apply to all levels of organizations and complexity depending on the amount of time and analysis they wish to devote to the process. A small business could use one or two levels of hierarchy and stay within the overall system structure. Extensive due diligence on deeper levels could also be applied, including outside experts and a range of analysis before a final determination is made in the prioritization and measures to protect the organization are decided upon.

Objective 1, Prioritize Risk - Steps 1-4

When an organization can prioritize risk, it can be aware of those risks that present the most significant impact at any given point in time based on the organization's unique characteristics and risk tolerance. With a careful and thorough review across a range of exposures a more holistic determination can be constructed of the highest impact risk scenarios. By analyzing and determining an impact, priority risk scenarios can be plotted on a risk map giving leadership an opportunity to allocate resources in addressing what is most critical. With clear priorities and executive directive, the organization is now able to achieve greater resiliency and sustainability as it pursues its objectives. Objective 1 (Prioritize Risk) does not address the techniques involved in protecting the organization or executing and administering the treatment of risk, but these activities in Objective 2 (Protect the Organization) all rest upon being able to effectively identify and analyze risk. Prioritization of risk, which includes identification and analysis, is paramount and must be addressed to effectively manage risk. Through practical application of risk identification and analysis with a framework that can encompass risk in general, skills are developed that can be used to address and adapt to future unknown or emerging risk scenarios as they become apparent.

Step 1, Logical Classification

There are a variety of methods that can be used to identify exposures. Once identified, they can be broken into logical classifications. “The use of logical classifications is a systematic way of classifying and categorizing exposures and the perils, hazards, and/or losses arising from exposures, so they can be effectively analyzed, controlled, transferred, and financed.” (The National Alliance Research Academy Risk and Insurance Studies, 2008)

The four logical classifications of exposures relied upon include Property, Liability, Human Resources, and Net Income. At this stage a determination must be made as to whether the exposure exists for the subject/entity or not. Without an exposure it is presumed there can be no loss. Example there is no exposure for auto liability without an auto.

A list of exposures can be made at an elevated level or can be refined to more specific detail. Example of exposure identification broken down from a top-level classification to sub classification detail.

1. Property
    a. Intangible
        i. Data
            l. Protected/Confidential Information
                a. Protected Health Information (PHI)
                b. Personally Identifiable Information (PII)

Once exposures are identified and classified, they can be defined in more detail and linked to key causes of loss.

Step 2, Exposure Variables

It is not adequate to merely specify if an exposure exists or not. It must be better defined and clarified. Too often exposures are dismissed or thought of as low priority without the realization of their significance. This is where the concept of exposure variables comes in. Key characteristics and detailed description that best define and bring clarity to the exposures identified Step 1. An exposure may be

disregarded as non-existent yet upon application of exposure variable analysis, it is defined to exist or to increase in significance.

As an example, consider a tenant that leases office space from a building owner. Although they do not own the building per the lease agreement they are required to insure the structure per contract. Thus, even though the tenant does not own a building the non-owned asset becomes an exposure for the tenant based on a contractual requirement. Legal, contractual risk transfer including indemnity can shift risk and change the existence of an exposure from negative to positive. Ownership and legal considerations are just one class of exposure variables that can impose a range of liability and responsibilities arising out a given exposure.

Each exposure variable can alter the impact of the other exposure variables. All four classifications of exposure variables can be applied to any unique exposure. The result is clarity and definition of the exposure. Exposure variables information can also be significant in protecting an asset and in deciding the best techniques for risk control and insurance as they illustrate the characteristics of the exposure.

Step 3, Perils

Perils are causes of loss. These causes directly correspond to risk controls to minimize the frequency and/or severity and to the insuring agreements that would be triggered by these perils as part of the risk finance. Understanding what can cause a loss to a given exposure is central to being able to determine its vulnerability. An exposure that is more vulnerable to loss could increase the impact to the organization.

Classification of perils can breakdown to include those related to Human beings, both on a micro and macro level. Other classifications include Mechanical/Chemical/Cyber-Physical, and Natural causes of loss.

Through a hierarchy of perils, exposures can be related to their key causes of loss. Each exposure has its own set of perils that apply to it. A peril can apply to more than one exposure and any exposure can have multiple perils. Understanding what is the cause of damage to organizational assets and operations allows the selection of risk control techniques and insurance to address and trigger based on realistic loss scenarios.

Step 4, Impact

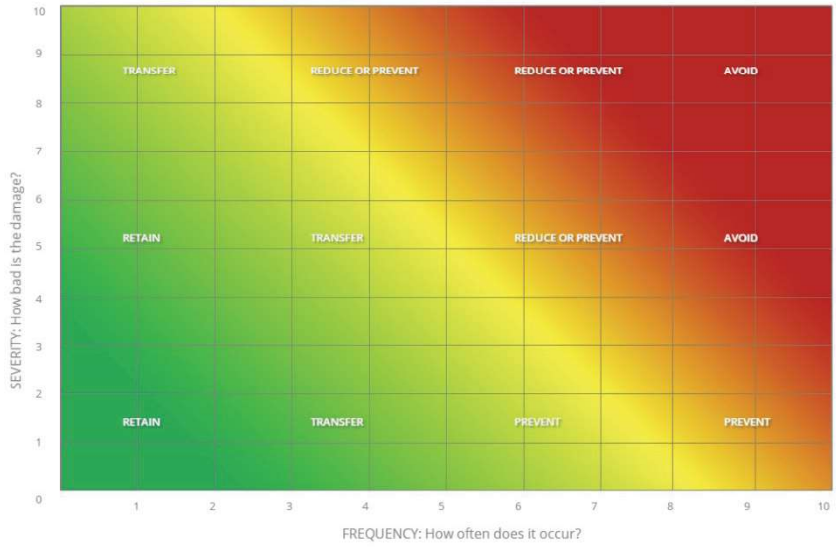
Ultimately an impact must be determined for each risk scenario arising out of the review of exposures, their exposure variables, and key causes of loss. (Steps 1,2 and 3). The impact is the basis in determining priorities out of the identified exposures. The higher the impact the more critical the risk scenario. Allocating resources towards the most critical risks is the best way to protect the organization based on known data. Ultimately, all risk can be refined to frequency and severity. How often is the risk event likely to happen and when it does, how bad is the damage.

The Risk Meter (a type of risk map) is a visual representation, providing a way to illustrate2 and discuss potential risk management priorities. Risk scenarios are prioritized, and the organization can now focus on Objective 2 (Protect the Organization). The risk meter itself indicates potential treatments for risk scenarios based on frequency and severity. At minimal frequency and severity retaining the loss makes sense. The severity of the loss is minimal, and it is not likely to happen. If it does occur, retaining the cost of the loss and its impact would be easily absorbed without disruption or major impact. As we move up the scale we can use other techniques include the use of insurance to transfer the cost of a potential loss from the company's balance sheet to the insurance carrier. At the highest level, would be a recommendation to avoid because the impact is too great and not worth the risk. Unfortunately, in today's business environment, technology risk is unavoidable, which further accentuates the value of a framework to address overall risk.

Certain factors influence frequency and severity. In determining your final risk score these factors modify the frequency and severity ratings that lead to a risk score, which is then plotted on the risk meter. The risk meter (Figure 2) gives a visual representation for the risk impact scores of key risk scenarios. On this XY chart the Y axis is the Severity score and the X axis is the Frequency score. The organization can

then agree to focus on of list of actionable priorities which will be addressed in Objective 2 (Protect the Organization).

FIGURE 2
THE RISK METER



Risk Dynamics

Risk Dynamics are modifying factors that affect and aide in the determination of the scoring for frequency and severity. These factors influence the ultimate risk score. By considering these factors the accuracy of the impact score is increased. The resources allocated in protecting the organization are maximized when focused on the risks that pose the greatest threat. Figure 3 explains a proposed Risk Impact Score Development.

FIGURE 3
RISK IMPACT - SCORE DEVELOPMENT

Risk Dynamics Affecting Severity

Risk Dynamics modify severity. The premise of Duration is that the length of a risk impact and the time from impact to mitigation affects the severity of a risk event. An example might be an electrical grid where restoring electricity after a storm could start with key facilities and work its way to repairing lines to individual customers.

Replacement of major generation stations and specialized equipment that provides electricity for a larger portion of the electrical grid can take much longer and increase the severity of the event. The longer the duration the more damage can compound and increase.

The premise of Velocity is, the more time an entity can have in perceiving or forecasting the impact of a risk event the more opportunity to minimize the severity. This is the emphasis of early warning regarding natural disasters, but could apply to risk in general.

The premise of Vulnerability is the more vulnerable an entity is to a given risk the more sever the event can be as there is less defense. Vulnerability is modified by threat force vs. control strength. How strong an entity's risk control program is in reducing the severity of a loss the less vulnerable they will be. The threat force is the strength to cause damage. Effectiveness of control strength can vary depending on the power of the threat force. The motivation and capability of the threat force/community vs the strength of risk control leads to a vulnerability score.

Direct and Indirect Loss

Severity would include both direct and indirect losses. Average loss and maximum loss affecting an organization can be reviewed to determine a realistic score for severity. Understanding direct and indirect loss gives valuable insight into the scope of potential harm arising out of any given risk scenario.

Consider the owner of a very early factory who had purchased fire insurance and suffered a total loss (Direct Loss). He had an insurance policy to cover the loss and was confident in the assurance that he would be reimbursed for his building and contents by the insurance company. During the period of restoration, he found over time that his employees had found other jobs and his customers had found other suppliers. Even though his building and contents were replaced the loss of income and the ramifications of the indirect losses arising out of the direct loss to his building and contents resulted in shutting his doors permanently. Indirect loss can also be described as time element as the length of time affects the amount of damage.

Indirect loss can arise outside of direct loss. This can be considered contingent in nature. An example, could be the distributed denial of service attack against Dyn in October of 2016 where reliant companies suffered loss due to the inability of customers to access their websites. Not because of direct loss to the website itself, nor to the hosting companies but to an intermediary. "Unfortunately, during that time, internet users directed to Dyn servers on the East Coast of the US were unable to reach some of our customers' sites, including some of the marquee brands of the internet" (Dyn Blog, 2016). As technology is highly integrated an indirect loss can happen regardless of a direct attack causing loss of profit and extra expenses. Consideration of both direct and indirect losses is required to assess the total spectrum of risk severity.

Risk Dynamics Affecting Frequency

Risk Dynamics also modify frequency. Vulnerability effects both the Severity of a loss as well the Frequency of a loss. Exposure is based on the effectiveness of an organization's risk control. A strong risk control program shows a more mature organization focused on sustainability. This information is a significant component in insurance underwriting in determining a more favorable risk. An effective risk control program can directly relate to historical loss results.

A known misconception concerning risk is that accidents mainly occur in specific intervals. An accident that has just occurred is less likely to happen again in a small time period. One example is a 100-year flood. The U.S. Geological Survey "…reminds the observer that a rare flood does not reduce the chances of another rare flood within a short time period." (USGS, 2016)

Workers compensation insurance can be experience rated. This experience rating is based on the history of losses for one company compared to the losses of other companies of similar size, in the same industry. (WCIRB, 2017) A rating is determined based on expected losses vs the actual losses experienced by the company over a certain period. A higher score corresponds to an above average loss experience. If the losses are below average a lower score is issued. This experience modification factor directly affects the cost of workers compensation premiums for employers. The formula to determine the experience rating places greater weight on the frequency of claims, which is believed to be a more accurate predictor of future claims and may be more under the control of the employer.

"Most experts agree that unsafe behaviors are the greatest source of losses, and that controlling unsafe behaviors will have the greatest impact on frequency." (The National Alliance Research Academy

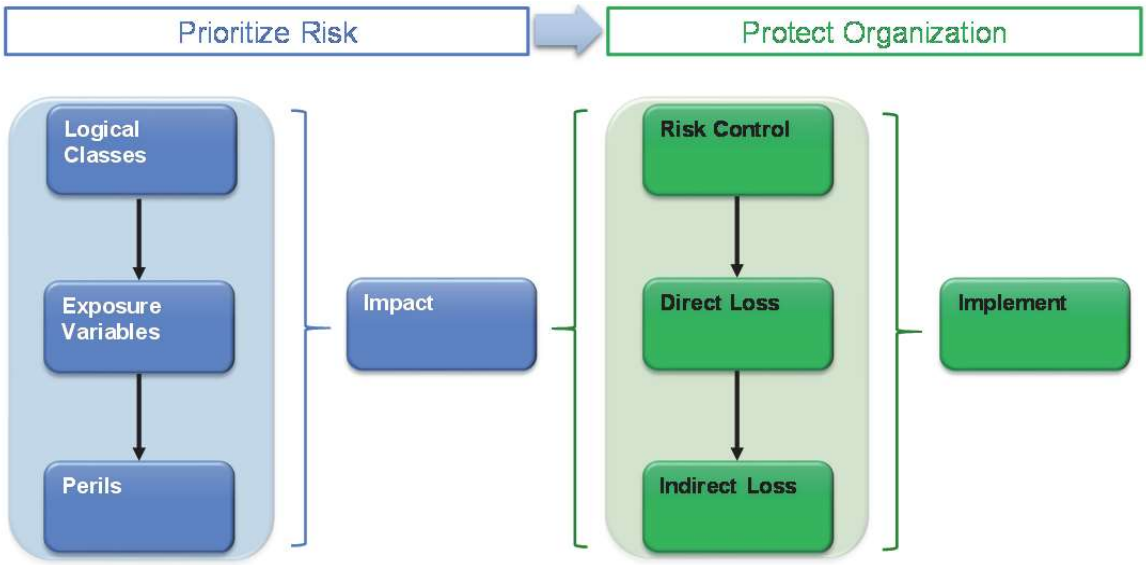
Risk and Insurance Studies, 2014) Lack of risk control is believed to ultimately drive frequency which leads to increasing insurance premiums over time due to frequent losses.

In considering these key factors we can arrive at a risk score based on the frequency vs. severity and the modifying factors that contribute to that determination. Following this process an organization can arrive at risk score for any given risk scenario. The accuracy of the risk score is determined by the relevancy and accuracy of contributing data. Ultimately the risk scenario scores are placed on a risk meter.

Objective 2 (Protect the Organization)

The second objective is about protecting the organization based on the risk priorities identified and analyzed in Objective 1 (Prioritize Risk). This consists of controlling risk, financing risk and the administration of selected plans and programs. This is where the organizations can act upon identified priorities for the purpose of protecting sustainability and resiliency. This "diagnose and then prescribe" idea is the correct approach. This is where we match up the identified risk priorities with risk control and risk finance techniques as illustrated in Figure 4.

FIGURE 4
PRIORITIZED RISK MATCHED WITH RISK CONTROL AND FINANCE TECHNIQUES



Step 1, Risk Control

Risk control is any conscious action or inaction, to minimize at the optimal cost, the probability, frequency, severity, or unpredictability of loss. (The National Alliance Research Academy Risk and Insurance Studies, 2014) Risk control can take place before the loss or after the loss. Many frameworks are designed around the control of risk, including those based on compliance. Frameworks for risk control include areas such as safety, security, human resources, continuity, and others. Many of these frameworks are well developed and continue to evolve. The detail of any given risk control plan will not be illustrated in this article. The aim of this section is to put risk control plans in the context of a larger framework and connect it to the other steps in this process.

Risk control rests on effective completion of Objective 1 (Prioritize Risk). Understanding how a given exposure is defined and the key perils that create a loss directly tie into the measures needed to minimize and prevent loss. By analyzing historical data, how loss occurs, environmental conditions where loss

occurs, learning from previous incidents, sharing data and predictive analysis, risk control measures adapt and evolve to meet changing and emerging risks.

Determining the vulnerability of an organization is part of determining the impact of a given risk scenario. By doing this identification, the effectiveness of risk controls would need to be reviewed. The results of that review can be tied to improving the risk control program moving forward.

Key steps of the risk control program would include avoidance, prevention, reduction (pre-loss and post-loss) and transfer. Multiple techniques can be employed together. (Certified Risk Managers International, 2010)

With cyber risk, increased complexity and the instantaneous transfer of information are present. Utilization of artificial intelligence and analysis to comprehend and make real-time decisions are viable options in comprehending this complexity. Human endeavors requiring technology to extend its capabilities may depend on another set of technology systems to control the risk resulting from the use of these technologies.

Risk control directly ties to insurance underwriting. The insurance application itself is a questionnaire regarding the company's risk control and behavior. From an insurance carrier perspective risk is speculative in nature. To make a profit underwriting discipline requires the examination of the risk controls and behavior of an organization to determine the profitability of the account. Risk control affects the likelihood and severity of loss and the pricing of insurance.

Step 2, Risk Finance Direct Loss

Guarantees in mitigating 100% of risk are extremely hard to find, fraudulent or impossible to achieve. From the SEC regarding mutual funds past performance: "That's why the SEC requires funds to tell investors that a fund's past performance does not necessarily predict future results." (U.S. Securities and Exchange Commission, 2010) Just because an event has historically not happened or not likely to happen in the foreseeable future does not guarantee it will not happen. Since change is the only guarantee, the need to finance potential losses along with efforts to control risk round out the most comprehensive approach to effective risk management when they are implemented.

Risk finance techniques can include retention and transfer of risk. Regardless of whether an organization chooses to transfer risk to an insurance company the organization will be responsible for the financial consequences of loss. This is called retention, where the organization retains the loss. This can be a passive or unconscious approach or an active retention. For most businesses the transfer of a financial loss to an insurance company is critical as a financial backstop. As cyber risk has grown exponentially many companies and individuals have been caught off guard and forced to retain risk because they did not have the appropriate insurance.

Early insurance in the United States started with the peril of fire. As property and casualty insurance evolved insurance carriers struggled with the idea of all risk vs. named perils. All risk being coverage except what is specifically excluded, named peril specifically lists the causes of loss that trigger the policy. In speaking with an underwriter from the late 60's and 70's insurance companies were initially hesitant to offer all risk coverage. One influencing factor was a review of a list of over 360 perils. This raised a couple of issues. What if an agent fails to offer coverage for the correct peril affecting an insured? The other issue was the threat of lawsuits that would need to be defended by insurance companies offering errors and omissions insurance to cover licensed insurance agents. If the agent fails to identify and offer coverage for a peril that may give rise to a loss it could be considered malpractice. Eventually "all risk" property polices became the preferred standard, which was eventually renamed to open peril to avoid confusion that "all" was covered.

Both liability and property related insurance are triggered by covered causes of loss. Many insureds wish they could purchase an insurance policy with no exclusions that covers the entirety of risk. Unfortunately, almost all would fail at completing the massively extensive application and paying the exorbitant premium it would cost for the insurance policy. An effective insurance program is about putting together the right pieces to cover exposures and key causes of loss prioritized in Objective 1 (Prioritize Risk). As cyber liability insurance continues to evolve the number of policy forms and

endorsements have increased to over 125+. Each policy form has different terminology making the ability compare insuring agreements, terms, conditions, and exclusion more difficult for insureds. The most effective approach in selecting the correct insurance for any organization is to tailor and match the insurance coverage based on risk priorities and identified impacts.

The logical classes that are used to classify exposures in this model can be tied to applicable insurance. The perils identified in this model can also be used to correspond with applicable insurance coverage as they relate to an exposure.

One example is in property insurance where you have insurance for buildings (Table 1). You also have specific insurance policies for earthquake (a key peril affecting buildings in certain geographic areas). Both are linked up to the exposure classification of Property. One is focused on the peril of earthquake. Both policies cover buildings. This model as an integral part of this framework provides a convenient way to match insurance policies and insuring agreements with the logical classifications of risk.

TABLE 1
PROPERTY INSURANCE EXAMPLE

Exposure Classification	Exposure Type	Exposure Sub-Type	Perils	Insurance Policy
Property	Tangible	Building	Fire	Building & Business Personal Property Policy
Property	Tangible	Building	Earthquake	DIC, Earthquake Policy

Insurance coverage for an organization can primarily be broken into 1st party and 3rd party risks. 3rd party risk is associated with liability exposures and getting sued by a third party. All liability insurance focuses on the payment of legal defense fees and can include settlement. The key difference in these liability insurance policies is how they are triggered. There are many types of legal exposures. The remainder mostly falls into 1st party risks applying to the insured's own property. Property and Net Income exposures can be considered 1st party risks.

With a thorough review of exposures appropriate insurance coverage can be matched. This empowers the insurance buyer's ability to select the right insurance coverage as well as identify gaps in their insurance program.

Step 3, Risk Finance Indirect Loss

As indirect loss must be accounted for in determining severity, insurance for Net Income losses must also be addressed. Net income includes loss of profit and extra expenses. This can be referred to as time element and "is generally measured by adding the net profit and continuing expenses. The longer the time the revenue or expenses are affected, the greater the loss." (Richard G. Rudolph, 2012) An example would be a denial of service attack that shuts down an eCommerce website causing a loss of sales. Another indirect net income loss might be an earthquake in a foreign country that disrupts the supply chain for a manufacturer. That manufacturer relies on a specific distributor that sources its materials from the country affected by the earthquake. Even though the manufacturer was not affected directly their operations were disrupted by the indirect loss that affected the supplier they relied on.

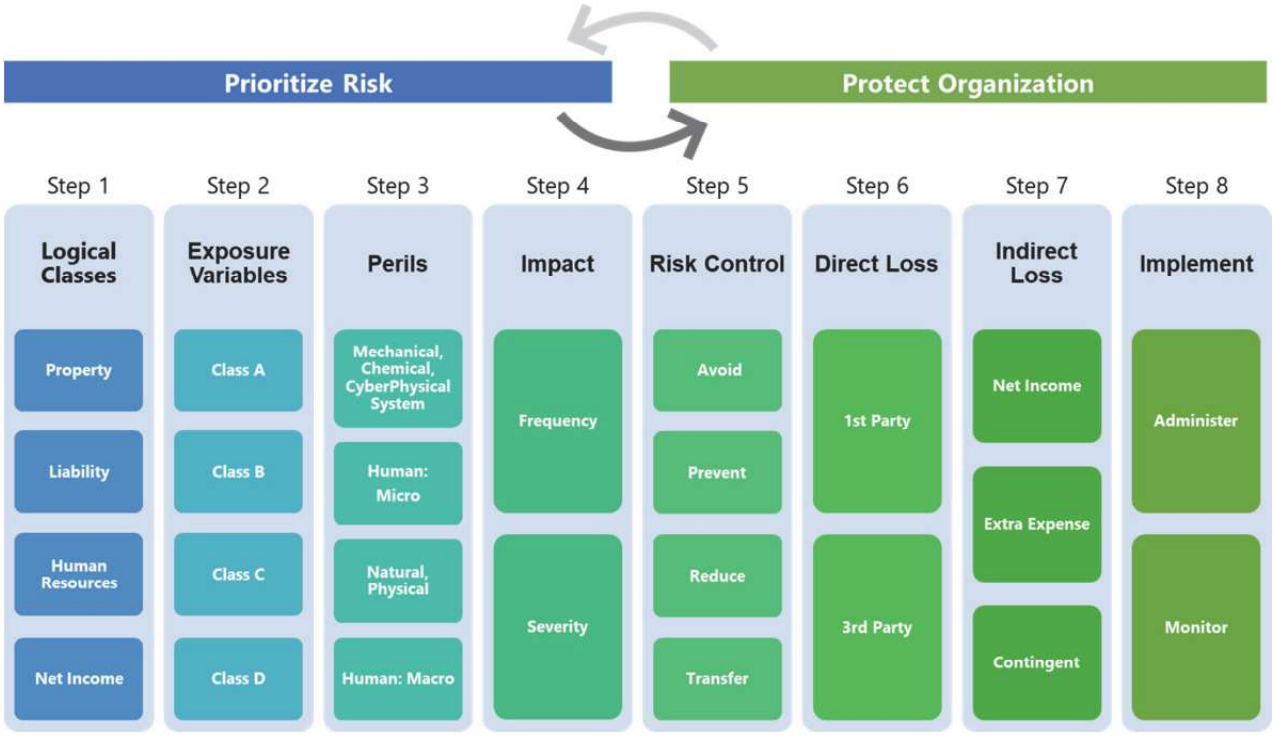
Insurance for indirect loss is applicable to both physical and cyber exposures. Even with insurance for direct loss without the ability to recover from indirect losses, including loss of profit and increased expenses following a loss, it may be difficult or impossible for an organization to recover.

Step 4, Risk Administration

Although there is immense value in the knowledge that comes through following this process, there will not be a reduction in risk unless the organization implements the risk control and risk financing

techniques (Figure 5). Understanding and deciding what to do is (steps 1-7 below) and the other is doing it (step 8). Ultimately, nothing gets done without leadership and many initiatives fail because the leadership did not incorporate the importance of risk management objectives into the culture of the organization. Good intentions are not enough. The significance of technology risk alone should sound the alarm. Obtaining a cultural balance by incorporating a holistic approach to reviewing risk and acting on risk management objectives is imperative.

FIGURE 5
IMPLEMENTATION OF RISK CONTROL AND FINANCING TECHNIQUES



Two ways of measurement in risk management are quantitative and qualitative analysis. Two basic ideas in determining metrics surrounding risk management include the Total Cost of Risk and a key question related to qualitative analysis.

Quantitative analysis is focused on using financial or statistical methodologies to calculate relative values. (Certified Risk Managers International, 2013) One method is The Total Cost of Risk. These are quantifiable costs associated with the process of managing risk. With this approach you would add the insurance premiums, retained losses (including insurance policy deductibles or retentions and losses that were not insured), risk management department costs, and outside consulting, services, and fees. The total cost of risk and the prioritized risk impact scores using this framework directly relate to each other. By comparing the results of practicing this risk management framework to the total cost of risk at two different points in time gives the opportunity to optimize and ultimately lower the total cost of risk for an organization.

From a qualitative standpoint a key question would be: "how do you measure the success of a non-event?". This is the value of effective risk management where the executive question could be asked: What is the value of the expense incurred in managing risk if no significant loss has occurred? There is no correct answer, but a starting point would be based on the growth and success of an organization over time. Profits, productivity, goodwill, reputation develop over time. The longer an organization can grow without a loss or uninsured/unmitigated loss the greater the organization could potentially become.

THE RISK CALCULATOR TOOL

This framework was developed based on work with 100 individuals across 20 verticals over a decade. Based on this interaction, the framework above has been developed along with a Risk Calculator software database tool based on the framework. In working with individuals, business, and non-profit organizations from a range of industries as a licensed property and casualty insurance agent, it became clear that not only an understanding of a holistic framework for risk management, but an automated tool to assist in executing the process was absent for most small and medium enterprises. Most do not have a risk manager on staff and the role of risk management is tasked to one or more executives or board members within the organization regardless of their expertise, job function or understanding of risk management. Many are functioning with little to no overall data on exposures facing the organization or how the current risk control and risk finance program are addressing exposures.

In closely held organizations of any size, the ultimate responsibility for the fact that risk management decisions may determine the existence of the company rests with the shareholders. These conscious or unconscious courses of action will be made regardless of the inside or outsourced resources that are employed, or the individual background, education and skill set of those responsible. The truth is that the components of this framework are applicable to organizations of any size, any industry at any level of sophistication.

If you take the entire spectrum of risk, there are periods of time where overall risk is increasing or more stagnant. In a period of accelerated risk, the importance for business leaders to understand and practice risk management becomes critical. That time is now. One example is a shift in the exploitation of vulnerabilities in evolving technology that has created an entire alternative economy of cybercrime. Legitimate enterprise must confront the reality of this cyber risk or fall in its wake.

FRAMEWORK TEST USING THE RISK CALCULATOR TOOL

The Risk Calculator Tool was designed to accelerate the practice of risk management and help to organize and create risk profiles based on unique characteristics. It does not employ the risk impact score currently. Perils find exposures. (Fire finds flammable material) Exposures are covered by insurance to protect against perils. (Buildings are covered by property insurance from the peril of fire) Insurance needs perils and exposures to define the coverage. (These three elements are interrelated). In beta stage, the Risk Calculator creates relationships between exposures, perils and insurance policies. Large amounts of Information can be entered, and multiple queries can be run based on the collected data.

By understanding the exposure and applicable perils you can define applicable insurance policies.

FIGURE 6
EXPOSURE TO POLICY - CONFIDENTIAL DATA SHOWING RELATED INSURANCE POLICIES

ExposureType	ExposureSubType	ExposureSubSubType	Exposure	MasterPolicyDef
Liability	Executive	ErrorsOmissions	LiaExErrProtectedDataTypesConfidentialData	Cyber Liability
Liability	Executive	ErrorsOmissions	LiaExErrProtectedDataTypesConfidentialData	Technology Errors & Omissions

By understanding a peril, you can find associated exposures.

Figure 7.
Perils to Exposures – Malicious Code showing related Exposures

PerilPerilClass	PerilPerilSub	PerilPeril	Exp2PerilExp	Exp2PerilExposureSubType	Exp2PerilExposureSubSubType	Exp2PerilExposure
MechanicalChemicalCyberPhysicalSystems	Digital	MCCPDiMaliciousCode	Liability	Employers	LegalIndustryCompliance	LiaEmLegContractual
MechanicalChemicalCyberPhysicalSystems	Digital	MCCPDiMaliciousCode	Liability	GeneralLiability	OperationsProducts	LiaGeOpeOngoingOperations
MechanicalChemicalCyberPhysicalSystems	Digital	MCCPDiMaliciousCode	Property	Intangible	Brand	PropInBraReputation
MechanicalChemicalCyberPhysicalSystems	Digital	MCCPDiMaliciousCode	Property	Intangible	Data	PropInDatProtectedDataTypesConfidentialData

By understanding an exposure, you can find associated perils.

FIGURE 8
EXPOSURE TO PERILS – BUILDINGS/STRUCTURES SHOWING RELATED PERILS

Exposure = Structures

Natural/Physical perils listed that are associated with structures.

Exp2Peril.Exp	Exp2Peril.Exp	Exp2Peril.Exp	Exp2Peril.Exposure	Ex	Peril.PerilClass	Peril.PerilSubClass	Peril.Peril
Property	Tangible	Structures	PropTaStrBuilding		NaturalPhysical	Earth	NPEaEarthquake
Property	Tangible	Structures	PropTaStrOutdoorProperty		NaturalPhysical	Earth	NPEaEarthquake
Property	Tangible	Structures	PropTaStrBuilding		NaturalPhysical	Earth	NPEaVolcanoes
Property	Tangible	Structures	PropTaStrOutdoorProperty		NaturalPhysical	Earth	NPEaVolcanoes
Property	Tangible	Structures	PropTaStrBuilding		NaturalPhysical	Earth	NPEaMudslideLandslide
Property	Tangible	Structures	PropTaStrOutdoorProperty		NaturalPhysical	Earth	NPEaMudslideLandslide
Property	Tangible	Structures	PropTaStrBuilding		NaturalPhysical	Earth	NPEaSinkhole
Property	Tangible	Structures	PropTaStrOutdoorProperty		NaturalPhysical	Earth	NPEaSinkhole
Property	Tangible	Structures	PropTaStrBuilding		NaturalPhysical	Earth	NPEaAvalanche
Property	Tangible	Structures	PropTaStrOutdoorProperty		NaturalPhysical	Earth	NPEaAvalanche
Property	Tangible	Structures	PropTaStrBuilding		NaturalPhysical	Earth	NPEaSubsidence
Property	Tangible	Structures	PropTaStrOutdoorProperty		NaturalPhysical	Earth	NPEaSubsidence
Property	Tangible	Structures	PropTaStrBuilding		NaturalPhysical	Earth	NPEaErosion
Property	Tangible	Structures	PropTaStrOutdoorProperty		NaturalPhysical	Earth	NPEaErosion

One key is how information of each of the components is organized into a hierarchal structure. From there it is cross referenced to supply responses to the above questions.

Use case: Law Firm - The firm was familiar with potential liability arising from a breach of client confidential and protected information that was utilized as part of their day to day operations. They did not have appropriate insurance for this exposure and the goal of the meeting was to gain familiarity with their exposures and applicable insurance. The first part of the discussion utilized exposure variables to determine the type, volume and potential legal ramifications regarding a breach of intellectual property, credit card data (the firm was accepting card payments for legal services that were being processed by a third party), medical information (related to legal matters surrounding physical injury) and location of information such as mobile devices. As this was documented it created greater clarity surrounding the identified exposure and helped to facilitate a more detailed discussion for both the legal and financial representatives present.

	LPID	LiabilityInsExecCyber.Exposure	InsGroup	InsSubGroup	CoverageType	CoverageSubType	CoverageSubSubType	
2		PropInDatProtectedDataTypesConfidentialData	Professional	Cyber	1st Party	Cyber Liability	REGULATORY ACTION AND PCI ENDORSEMENT	(1) Consum
3		PropInDatProtectedDataTypesConfidentialData	Professional	Cyber	1st Party	Cyber Liability	Privacy Notification and Crisis Management Expenses Coverage	(1) Privacy I
4		PropInDatProtectedDataTypesConfidentialData	Professional	Cyber	1st Party	Cyber Liability	Reward Expenses Coverage	Reward Exp
5		PropInDatProtectedDataTypesConfidentialData	Professional	Cyber	1st Party	Cyber Liability	E-Threat Expenses Coverage	E-Threat Ex
6		PropInDatProtectedDataTypesConfidentialData	Professional	Cyber	1st Party	Cyber Liability	E-Vandalism Expenses Coverage	E-Vandalism
7		PropInDatProtectedDataTypesConfidentialData	Professional	Cyber	1st Party	Cyber Liability	Consumer Redress Funds and Regulatory Fines	Consumer F

The firm was not familiar with the 1st party coverages available as part of a cyber liability insurance policy and specifically was interested in an insurance company they had previous experience with. Through use and customization of the Risk Calculator, the exposure of intangible property was queried resulting in detail of 1st party cyber liability insurance. The results of the query listed the insuring agreement based on the insurance company of preference, that were applicable to that exposure. This quickly facilitated a discussion surrounding intangible property and associated risk scenarios for both direct and indirect loss. As part of facilitating the discussion I was able to get agreement on some key risk priorities that needed to be addressed from a risk control and insurance standpoint. This is a brief example of utilizing the Risk Calculator to help facilitate the risk management discussion, improve efficiency, and increase understanding of cyber risk within the context of a holistic risk management framework.

CONCLUSION

In conclusion, training business leaders with a holistic understanding of risk management better equips organizations to understand, communicate and balance sales initiatives with risk management for more sustainability in an environment of accelerated risk particularly in the cyber world. The risk management framework helps to avoid a compartmentalized approach that creates too narrow of a focus and does not allow the risks facing the organization, including cyber risk, to be understood in a broader context. Through a holistic approach to risk management educated business leaders can make more informed decisions and advance the risk management discussion through a common framework able to tackle todays emerging risks. A new perspective and tools are required to ensure businesses incorporate cyber risk into decisions and initiatives in order to identify, evaluate and mitigate this risk. The framework presented here and tested through the tool developed provides businesses and business leaders with this new perspective and ways to deploy it throughout their organization.

REFERENCES

Alberts DS (2011). The agility advantage: a survival guide for complex enterprises and endeavors. DOD Command and Control Research Program, Washington, DC.

Beck, U. (1994/2003). *Risk Society: Towards a New Modernity.*Canadian Journal of Sociology, Volume 19, No. 4 pp. 544-547.

Bernstein, P. L. (2011). *Capital Ideas: The Improbable Origins of Modern Wall Street*. Wiley and Sons, Hoboken, NJ.

Certified Risk Managers International, The National Alliance for Insurance Education & Research, Control of Risk © 2010 All Rights Reserved.

Certified Risk Managers International, The National Alliance for Insurance Education & Research, Practice of Risk Management © 2013 All Rights Reserved.

Chiles, James (2002). Inviting Disaster: Lessons From the Edge of Technology. First Harper Business. New York, New York.

Collier ZA, DiMase D, Walters S, Tehranipoor M, Lambert JH, Linkov I (2014b) Cybersecurity standards: managing risk and creating resilience. Computer 47(9): 70-76.

Cox LA Jr (2008) Some limitations of ‘‘risk=threat x vulnerability x consequence’’ for risk analysis of terrorist attacks. Risk Analysis. 28:1749–1761.

Dimase, D., Collier, Z., Heffner, K. and Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. Environmental Systems Decisions. 35 (2), pp. 291-300.

Dyn Statement on 10/21/2016 DDoS Attack, Company News // Oct 22, 2016 // Kyle York, https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

Frick, D.E. (2012) The fallacy of quantifying risk. Defense AT&L 228:18–21.

Garaczi, I. (2013). Risk Models and Movements in Society. *Economics.* Vol 5.

Glaser, B.G. and Strauss, A.L. (1967,2000). The Discovery of Grounded Theory: Strategies for Qualitative Research. Transaction Publishers, New York, New York.

Griffy-Brown, C., Lazarikos, D. and Chun, M. S. (2016) How Do You Secure an Environment Without a Perimeter? Using Emerging Technology Processes to Support Information Security Efforts in an Agile Data Center. Journal of Applied Business and Economics. 18:1. pp. 90-102.

Kaplan S, Garrick BJ (1981) On the quantitative definition of risk. Risk Anal 1(1):11–27.

Lanyi, A. (2011). The End of Risk Society. *Culture and Science*. 9 (11/3) , pp. 7–13

Linkov I, Eisenberg DA, Plourde K, Seager TP, Allen J, Kott A. (2013b). Resilience metrics for cyber systems. Environ System Decisions. 33(4):471–476.

The National Alliance Research Academy Risk and Insurance Studies, Austin, Texas 2014, Risk Management Essentials, 2nd Edition, Digital Version, International Standard Book Number: 978-1-878204-77-6, https://nationalalliancebooks.com/, p39, 45, 217, 547, 548, 549, 558, 561, 562, 564

Olzak T (2013) Insider threats: implementing the right controls. TechRepublic, Originally published 21 Feb 2013. http://www.techrepublic.com/blog/it-security/insider-threats-implementingthe-right-controls/

Park J, Seager TP, Rao PSC, Convertino M, Linkov I (2012). Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Anal 33(3):356–367.

Richard G. Rudolph, PH.D., CPCU, ARM, ARP, APA, AIAF, AAM, Famous Reindeer Education Enterprises, LLC, Net Income Risk Management, 1st Edition, Digital Version, The National Alliance Research Academy Austin, Texas ©2012, ISBN# 978-1-878204-49-3, https://nationalalliancebooks.com/

Strauss AL, Corbin J. Basics of qualitative research: grounded theory procedures and techniques. Thousand Oaks (CA): Sage Publications; 1998.

Teng K, Thekdi SA, Lambert JH (2012) Identification and evaluation of priorities in the business process of a risk or safety organization. Reliab Eng Syst Saf 99:74–86.

Teng K, Thekdi SA, Lambert JH (2013) Risk and safety program performance evaluation and business process modeling. IEEE Trans Syst Man Cybern A 42(6):1504–1513.

U.S. Department of the Interior | U.S. Geological Survey , Page Contact Information: Howard Perlman Page Last Modified: Friday, 09-Dec-2016 13:21:20 EST, URL: http://water.usgs.gov/edu/100yearflood.html

U.S. Securities and Exchange Commission, Fast Answers, Mutual Funds, Past Performance, Modified: July 28, 2010, https://www.sec.gov/fast-answers/answersmperfhtm.html

Vasvari, T (2015). Risk, Risk Perception, Risk Management – a Review of the Literature. Public Finance Quarterly ν 2015/1 29.

The WCIRB, Experience Rating Plan Changes in 2017 — California's New Variable Split Point Experience Rating System, Accessed 21-Dec-2017, https://www.wcirb.com/rating2017

APPENDIX 1
DEFINITIONS

TABLE 2
DEFINITION TABLE

Term	Definition
Exposure	An asset or operation that may lead to an adverse financial consequence (an activity or resource; people and assets)
Exposure Variable	Attribute that further defines and describes an exposure
Peril	A cause of loss
Hazard	A condition or circumstance that may give rise to a loss from a given peril
Frequency	The number of losses occurring in a given time period
Severity	The dollar amount of a given loss or the aggregate dollar amount of all losses for a given period
Velocity	Perceptible speed of impact of a risk event
Duration	Length of time from impact to mitigation of a risk event
Risk Dynamics	Modifying factors that impact the severity and/or frequency of a risk event
Risk Financing	The acquisition of internal and external funds to pay losses at the most favorable cost
Risk Control	Any conscious action or inaction to minimize at the optimal cost, the probability, frequency, severity, or unpredictability of loss
Retention	Internal funds used to pay losses
Insurance Transfer	Using external funds to finance risks from one entity to another in exchange for payment