Quantitative Security

Colorado State University

Yashwant K Malaiya

CS 559

Risk and its components

CSU Cybersecurity Center
Computer Science Dept

FAQ

- Questions from last week
- The GTA will briefly address some of these.
- You can send your questions to

  cs559@cs.colostate.edu

Today

- Risk and its components
  - Visualization using Risk matrix
  - FAIR
- Insurance

Risk: Formal definition

Definition: The Risk due to an adverse event e_i is

$$Risk_i = Likelihood_i \times Impact_i$$

- $Likelihood_i$: Probability of the adverse event i occurring within a specific time-frame.
  - The time-frame is often chosen to be a year. Note that the probability of an adverse event happening depends on the duration of the time-frame.
  - Probability is a number between 0 and 1.
- $Impact_i$: The impact of the adverse event, measured in monetary terms.
  - Note that impact me be direct or indirect.
  - Common units are dollars (US$)#.

US$ is a common and convenient scale. Non-monetary losses, including human life, can be converted into US$, if you are a business or insurance company .

Colorado State University

Risk: Possible Actions

How to handle risk?

Example: Credit card fraud

- Risk acceptance
  - Ex: fraud cost paid through fees charged to merchants
- Risk mitigation
  - Ex: install anti-fraud technology, adds to costs
- Risk avoidance
  - downgrade high-risk cardholders to debit or require additional verification: lost time/business
- Risk transfer
  - buy cyber-insurance to cover excess losses

Risk as a composite measure

Formal definition:

- **Risk** due to an adverse event e_i

  $Risk_i = Likelihood_i \times Impact_i$

- A specific time-frame, perhaps a year, is presumed for the likelihood.
- $Likelyhood_i$ may be replaced by $frequency_i$, when it may happen multiple times a year.
- This yields the expected value. Sometimes a worst-case evaluation is needed.

In classical risk literature, the internal component of Likelihood is termed “Vulnerability” and external “Threat”. Both are probabilities. There the term “vulnerability” does not mean a security bug, as in computer security.

Risk as a composite measure

- Likelihood can be split in two factors

$$\text{Likelihood}_i = \text{P}\{\text{A security hole}_l \text{ is exploited}\}.$$
$$= \text{P}\{\text{hole}_i \text{ present}\}.$$
$$\text{P}\{\text{exploitation}|\text{hole}_i \text{ present}\}$$

- $\text{P}\{\text{hole}_i \text{ present}\}$: an internal attribute of the system.
- $\text{P}\{\text{exploitation}|\text{hole}_i \text{ present}\}$: depends on circumstances outside the system, including the adversary capabilities and motivation.
- In the literature, the terminology can be inconsistent.

Caution: In classical risk literature, the internal component of Likelihood is termed “Vulnerability” and external “Threat”. Both are probabilities. There the term “vulnerability” does not mean a security bug, as in computer security.

Annual Loss Expectancy (ALE)

Note the terminology is from the Risk literature.

- Single loss expectancy (SLE)

  SLE = AV x EF,

  - AV is the value of the asset. EF is exposure factor which describes the loss that will happen to the asset as a result of the threat, expressed as fractional (or %) value.
- Annual loss expectancy (ALE)

  ALE = SLE x ARO

  - Where ARO is Annualized rate of occurrence.
- Example: Asset value is $100,000, exposure factor is 30%, and ARO is 0.5 (once every two years). Thus
  - ALE = ($100,000 x 0.30) x 0.5 = $15,000.
- Note that ALE is essentially what we term as “risk”, with an annual time frame.

Annual value of the countermeasure

Cost/benefit analysis of countermeasures

- A countermeasure reduces the ALE by reducing one of its factors.

COUNTERMEASURE_VALUE

= (ALE_PREVIOUS – ALE_NOW) – COUNTERMEASURE_COST

Where ALE_PREVIOUS: ALE before implementing the countermeasure.

ALE_NOW: ALE after implementing the countermeasure

COUTERMEASURE_COST: *annualized* cost of countermeasure

- The COUNTERMEASURE_VALUE should be positive.

Likelihood & Impact scales

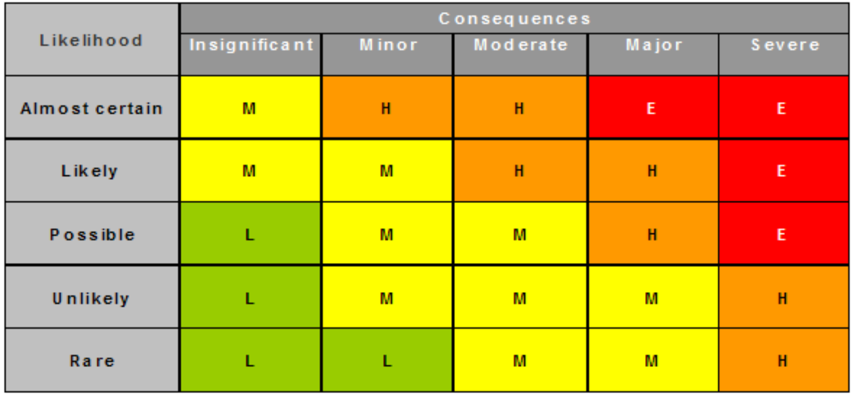
- Quantitative or descriptive levels
  - Number of levels may depend on resolution achievable
- Scale: Logarithmic, Linear or combined
  - A logarithmic scale is natural when the numbers involved vary by several orders of magnitude.
- Risk = Likelihood x Impact
  - May be rewritten as

    Log(Risk) = Log(Likelihood) + Log(Impact)
- If the term “Score” is proportional to Log value
  - Risk score = Likelihood score + Impact score
  - Adding scores valid if scores represent logarithmic values.
  - Example:
    - Likelihood = 10%, impact = $100,000 ⇒ **Risk = $10,000**
    - Scores: Log(0.10) = -1, log (100000) = 5 ⇒ **Risk score = 4**

$10^2 = 100$
$\text{Log}_{10}\ 100 = 2$
Log implies base 10, if not specified

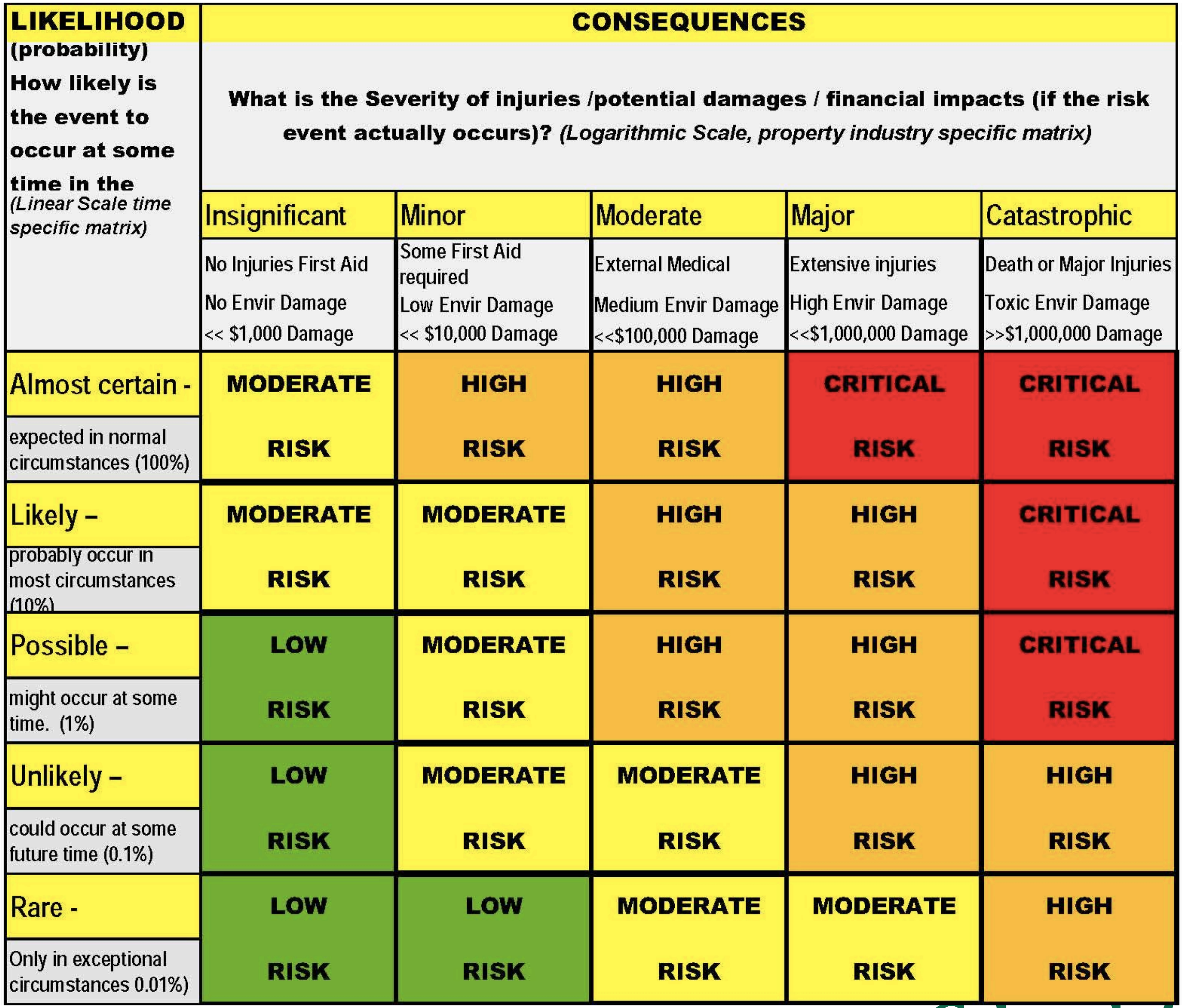
Risk Matrix

- Likelihood and Impact divided into levels
  - Each level quantitatively/qualitatively defined
- Cells marked by the overall risk
  - Low, Medium, High, Extreme etc.
- *Equal risk regions* along the diagonal, valid provided score scales are logarithmic.



Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

Risk Matrix: Example



LIKELIHOOD **(probability) How likely is the event to occur at some time in the** *(Linear Scale time specific matrix)*	**CONSEQUENCES**				
	What is the Severity of injuries /potential damages / financial impacts (if the risk event actually occurs)? ***(Logarithmic Scale, property industry specific matrix)***				
	Insignificant	Minor	Moderate	Major	Catastrophic
	No Injuries First Aid No Envir Damage << $1,000 Damage	Some First Aid required Low Envir Damage << $10,000 Damage	External Medical Medium Envir Damage <<$100,000 Damage	Extensive injuries High Envir Damage <<$1,000,000 Damage	Death or Major Injuries Toxic Envir Damage >>$1,000,000 Damage
Almost certain - expected in normal circumstances (100%)	**MODERATE RISK**	**HIGH RISK**	**HIGH RISK**	**CRITICAL RISK**	**CRITICAL RISK**
Likely – probably occur in most circumstances (10%)	**MODERATE RISK**	**MODERATE RISK**	**HIGH RISK**	**HIGH RISK**	**CRITICAL RISK**
Possible – might occur at some time. (1%)	**LOW RISK**	**MODERATE RISK**	**HIGH RISK**	**HIGH RISK**	**CRITICAL RISK**
Unlikely – could occur at some future time (0.1%)	**LOW RISK**	**MODERATE RISK**	**MODERATE RISK**	**HIGH RISK**	**HIGH RISK**
Rare - Only in exceptional circumstances 0.01%)	**LOW RISK**	**LOW RISK**	**MODERATE RISK**	**MODERATE RISK**	**HIGH RISK**

Example:

Likely x Moderate
= (10/100) x $100,000
= $10,000 High

Scales

Note the use of logarithmic scales.

Likelihood	
Almost certain	≈ 100%
Likely	≈ 10%
Possible	≈ 1%
Unlikely	≈ 0.1%
Rare	≈ 0.01%

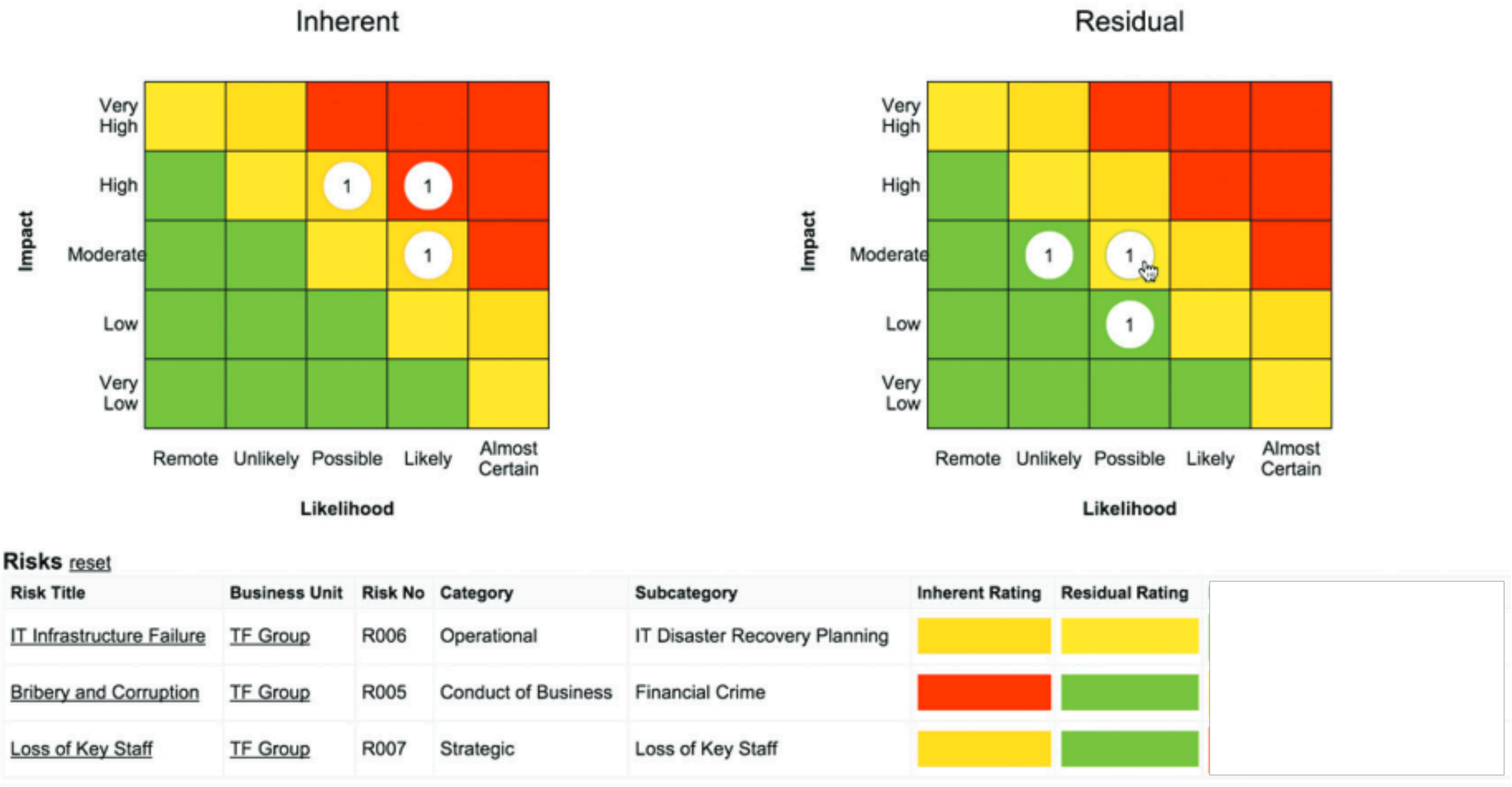
Consequence	
Insignificant	<< $1,000
Minor	<< $10,000
Moderate	<< $100,000
Major	<< $1,000,000
Catastrophic	>> $1,000,000 death

Colorado State University

Advantages of Risk Matrices

- Visual representation of distribution of risks in a system.
  - Similar to "Heat Maps" for the stocks in a market
- Change in overall risk due to a system redesign can be visualized.
  - Attempt to move risks from red region to green region.
- Allow expert estimates to be used instead of exact numbers.
  - Calibration or training may be needed to make estimates more accurate.

Visualizing Risk Reduction



Risks reset

Risk Title	Business Unit	Risk No	Category	Subcategory	Inherent Rating	Residual Rating
IT Infrastructure Failure	TF Group	R006	Operational	IT Disaster Recovery Planning	🟨	🟨
Bribery and Corruption	TF Group	R005	Conduct of Business	Financial Crime	🟥	🟩
Loss of Key Staff	TF Group	R007	Strategic	Loss of Key Staff	🟨	🟩

RISK MANAGEMENT FOR FINANCIAL SERVICES

Limitations of Risk Matrices

The main limitations of Risk Matrices arise because

- Limited resolution: continuous to discrete scales
- The scales are generally logarithmic
- May rely on subjective judgement, which may not be accurate.

- Cox, L.A. , ‘What’s Wrong with Risk Matrices?’, Risk Analysis, April 2008, Vol. 28, No. 2, pp. 497-512
- Julian Talbot, What's right with risk matrices? 2018

RAMCAP Framework

- Following Sept 11, 2001, ASME (formerly known as the American Society of Mechanical Engineers) convened more than one hundred industry leaders, at the request of the White House, to define and prioritize the requirements for protecting USA’s critical infrastructure.
- Recommendation: a risk analysis and management process to support decisions allocating resources to initiatives to reduce risk.
- Risk Analysis and Management for Critical Asset Protection (RAMCAP, RAMCAP Plus)
- Applicable to any type of risk: terrorism, dam bursts, ..

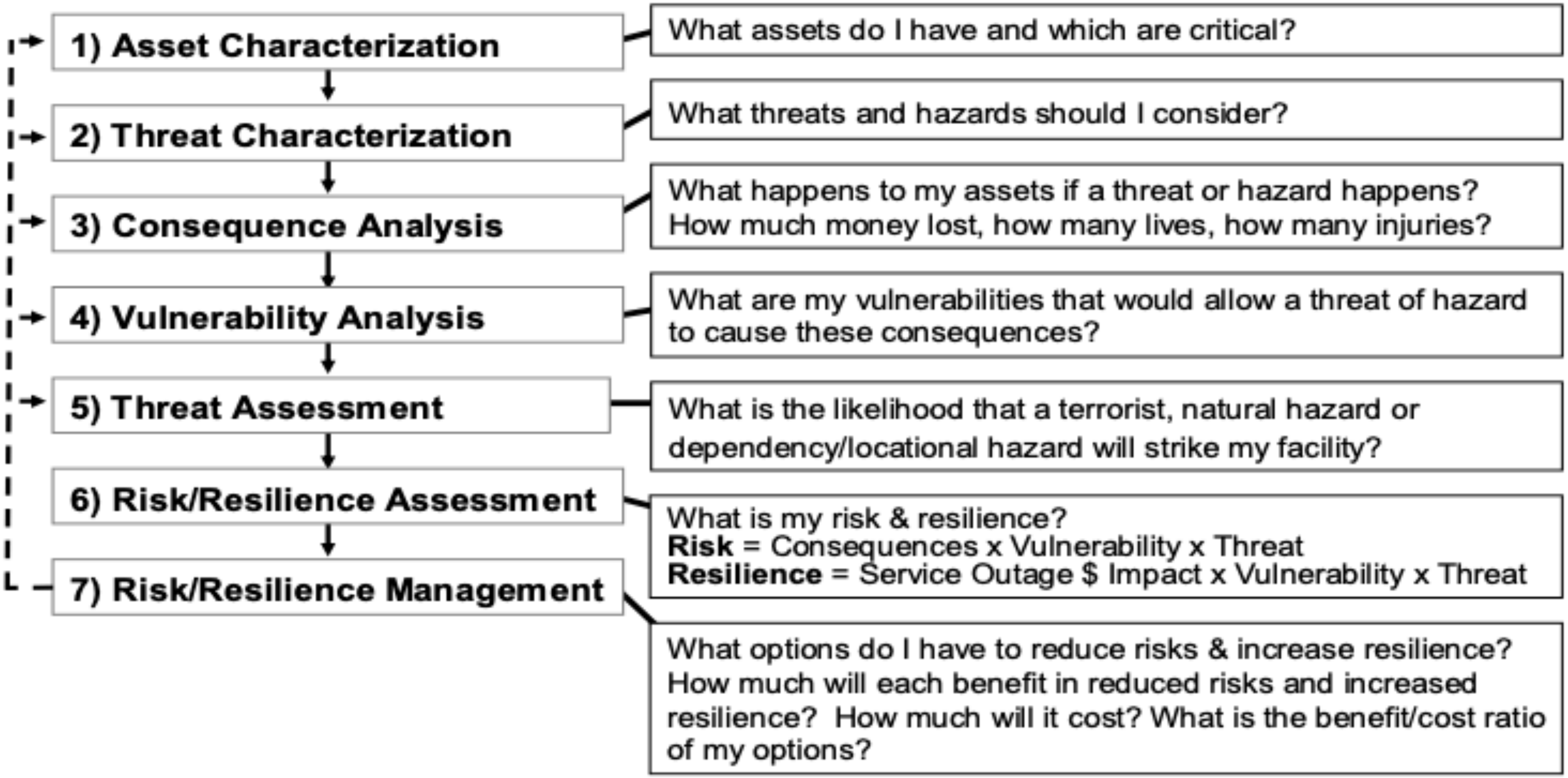
ALL-HAZARDS RISK AND RESILIENCE Prioritizing Critical Infrastructures Using the RAMCAP PlusSM Approach, 2009

Colorado State University

RAMCAP: Risk and Resilience Defined

- Risk = Threat x Vulnerability x Consequence
  - Resilience is the ability of an organization, facility or asset to function despite and during an attack or failure or to restore functionality in very short time.
  - $\text{Resilience}_{\text{Owner}}$ = Lost Net Revenue x Vulnerability x Threat
  - $\text{Resilience}_{\text{Community}}$ = Lost Community Economic Activity x Vulnerability x Threat

The 7-step RAMCAP Plus Process



1) Asset Characterization

What assets do I have and which are critical?

2) Threat Characterization

What threats and hazards should I consider?

3) Consequence Analysis

What happens to my assets if a threat or hazard happens? How much money lost, how many lives, how many injuries?

4) Vulnerability Analysis

What are my vulnerabilities that would allow a threat of hazard to cause these consequences?

5) Threat Assessment

What is the likelihood that a terrorist, natural hazard or dependency/locational hazard will strike my facility?

6) Risk/Resilience Assessment

What is my risk & resilience?
Risk = Consequences x Vulnerability x Threat
Resilience = Service Outage $ Impact x Vulnerability x Threat

7) Risk/Resilience Management

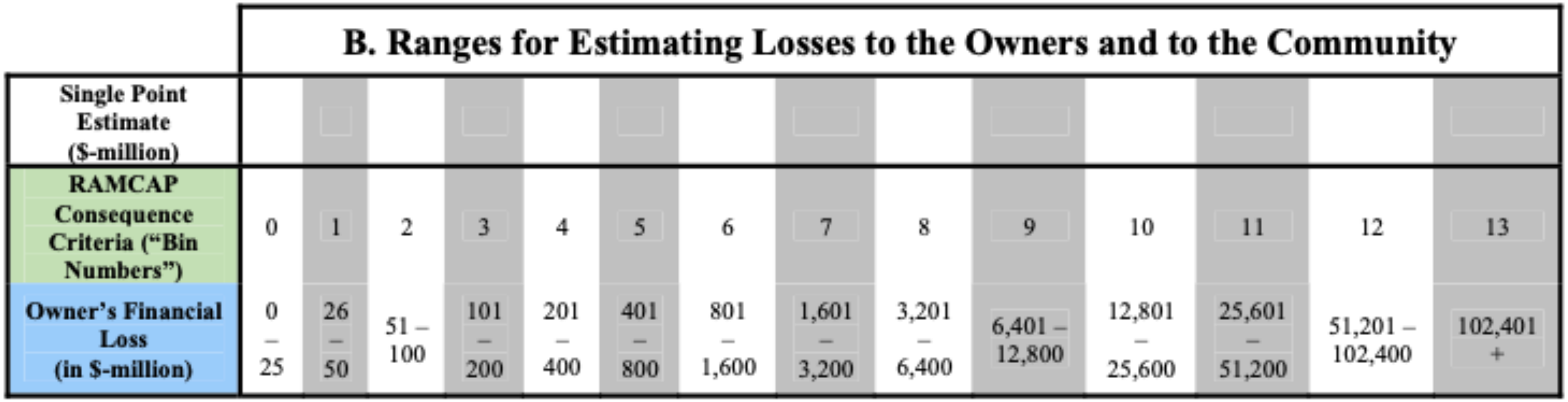
What options do I have to reduce risks & increase resilience? How much will each benefit in reduced risks and increased resilience? How much will it cost? What is the benefit/cost ratio of my options?

Risk Analysis and Management for Critical Asset Protection (RAMCAP Plus). Jerry P. Brashear, J. William Jones

The 7 Steps

- **1 – Asset Characterization** which assets, if damaged or destroyed, would diminish the facility’s ability to meet its mission.
- 2 – **Threat Characterization** the threat scenarios used are identified and described in enough detail to estimate vulnerability and consequences.
- **3 – Consequence Analysis** Consequence analysis identifies and estimates the worst reasonable consequences generated by each specific asset/threat combination.

The 7 steps



	B. Ranges for Estimating Losses to the Owners and to the Community													
Single Point Estimate ($-million)														
RAMCAP Consequence Criteria ("Bin Numbers")	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Owner's Financial Loss (in $-million)	0 – 25	26 – 50	51 – 100	101 – 200	201 – 400	401 – 800	801 – 1,600	1,601 – 3,200	3,201 – 6,400	6,401 – 12,800	12,801 – 25,600	25,601 – 51,200	51,201 – 102,400	102,401 +

- **4 – Vulnerability Analysis** estimates the likelihood of each specific threat or hazard to overcome the defenses of the asset to the level identified in the consequence estimate for that threat/asset combination.
  - Tools: Direct expert elicitation, Vulnerability logic diagrams (VLDs), Event trees (also called "failure trees")
  - Measured using bins

Colorado State University

The 7 steps

- 5- **Threat assessment** produces the probability (0.0 to 1.0) that a particular threat will occur in a given time frame.
  - Using historical data other other approaches
- 6 – **Risk and Resilience Assessment** using formulas
- **7 – Risk and Resilience Management** improving the risk level, resilience and reliability of the organization.
  - Decide whether the risk and resilience levels for each asset/ threat pair are acceptable;
  - develop countermeasures for each unacceptable asset/threat and estimate their investment and operating costs;
  - Evaluate the options using analysis

Criticism of *RISK* = *THREAT* × *VULNERABILITY* × *CONSEQUENCE* FRAMEWORK

Louis Anthony (Tony) Cox, Jr. “Some Limitations of “Risk = Threat × Vulnerability × Consequence” for Risk Analysis of Terrorist Attacks”, *Risk Analysis, Vol. 28, No. 6, 2008*

- Distortions Due to Use of Arithmetic Averages on Logarithmic Scales
- Improper granularity may be used
- Product of Expected Values Not Equal to Expected Value of Product
- Priority Ranking May Not Support Effective Resource Allocation
- “Threat” Is Not Necessarily Well Defined
- “Vulnerability” Can Be Ambiguous and Difficult to Calculate via Event Trees
- “Consequence” Can Be Ambiguous and/or Subjective

FAIR Framework

Factor Analysis for Information Risk: Developed by Jack Jones (Risk Management Insight LLC) 2005.

- Idea: Divide Risk in factors and then sub-factors which can be estimated.

Basis: Risk = Probably Loss Magnitude x estimated Loss Event Frequency

- Probably Loss Magnitude estimate using worst case loss
- Loss Event Frequency (LEF) = Threat Event Frequency x Vulnerability
- Vulnerability (Vuln) = Threat Capability x lack ofControl Strength
  - Threat Capability (Tcap) = The probable level of force that a threat agent is capable of applying against an asset (estimate)
  - Control strength (CS): The expected effectiveness of controls, over a given timeframe, as measured against a baseline level of force: estimate
- Threat Event Frequency (TEF): estimated
- “Multiplication” achieved by using Matrices.

An Introduction to FAIR, 2005

FAIR Framework: 4 Stages

Stage 1: Identify Scenario Components

- *Identify asset at risk:*
- *Identify the threat community: externa/internal*

Stage 2: Evaluate Loss Event Frequency

- *Threat Event Frequency (TEF):* probable frequency, within a given timeframe

TEF Ratings	Description
Very High (VH)	>100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year
Low (L)	Between .1 and 1 times per year
Very Low (VL)	<.1 times per year (less than once every 10 years)

An Introduction to FAIR, 2005, archived

FAIR: *Threat Capability*

- *Threat Capability (Tcap):* capability of the attacker to conduct the attack

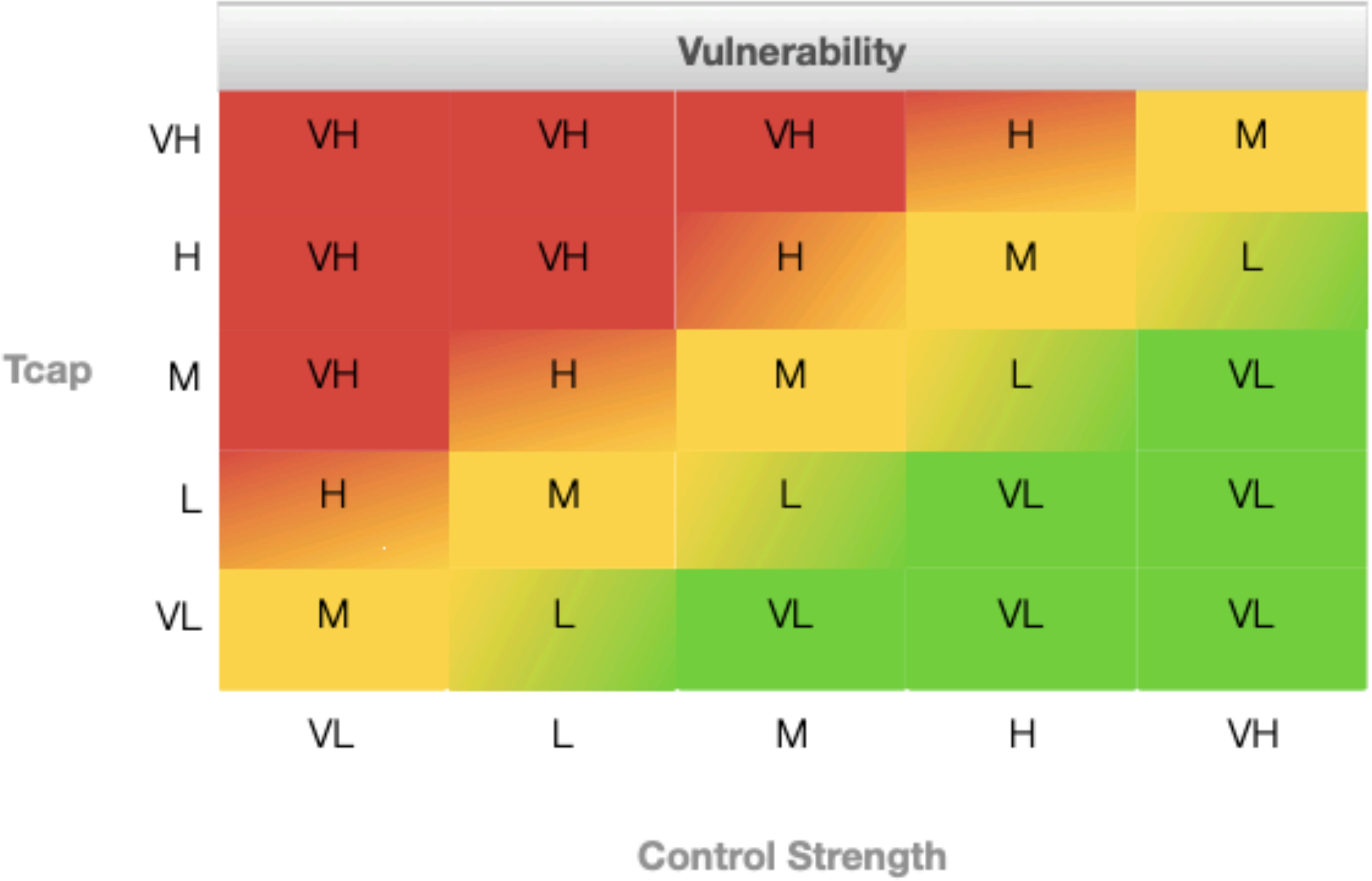
Tcap rating	Description
Very High (VH)	Top 2% when compared against the overall threat population
High (H)	Top 16% when compared against the overall threat population
Moderate (M)	Average skill and resources (between bottom 16% and top 16%)
Low (L)	Bottom 16% when compared against the overall threat population
Very Low (VL)	Bottom 2% when compared against the overall threat population

FAIR: Control Strength

- *Estimate Control Strength (CS):* FAIR defines this as the expected effectiveness of controls, over a given timeframe.

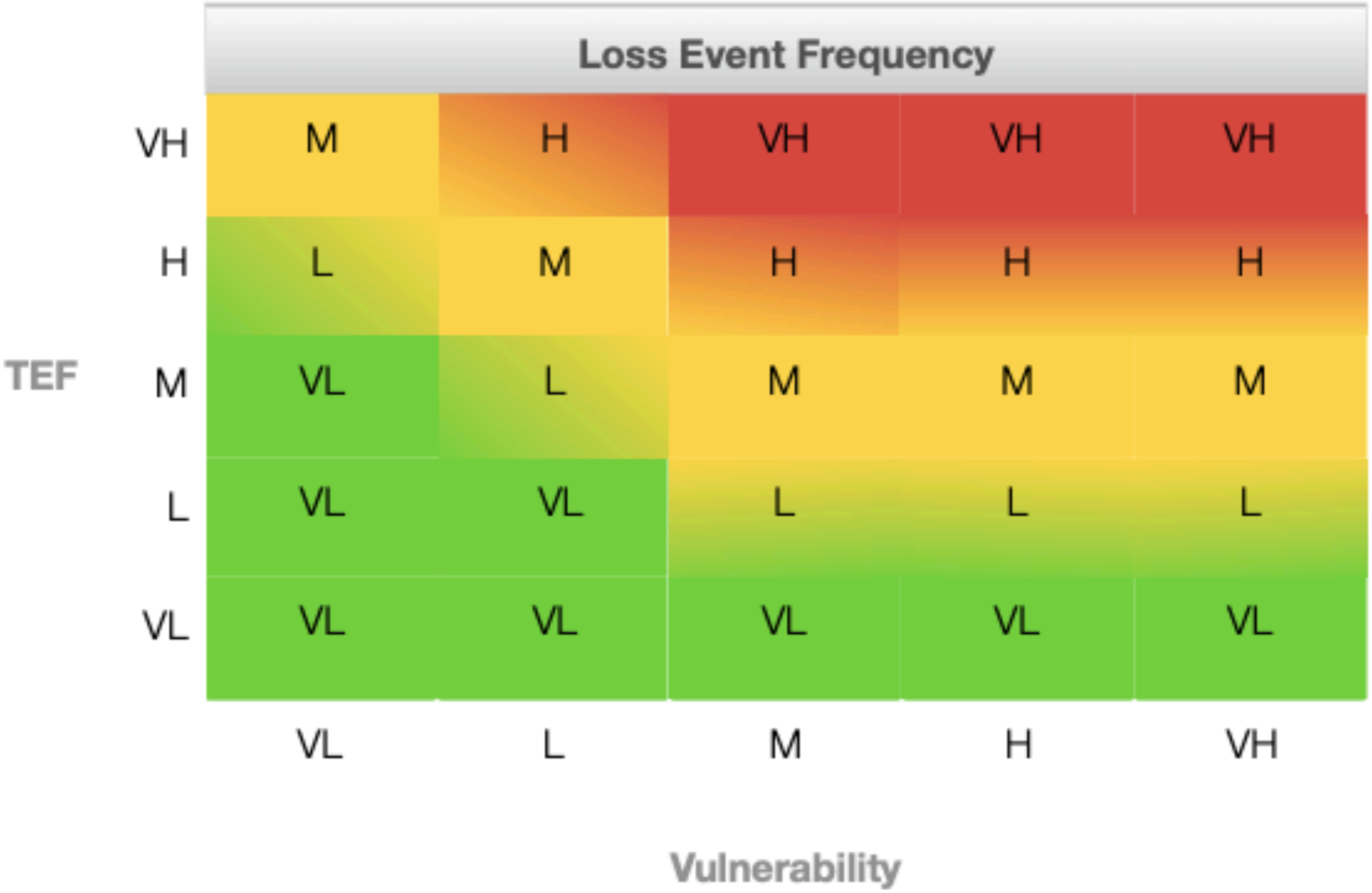
Control Strength rating	Description
Very High (VH)	Protects against all but the top 2% of an avg. threat population
High (H)	Only protects against bottom 16% of an avg. threat population
Moderate (M)	Protects against the average threat agent
Low (L)	Only protects against bottom 16% of an avg. threat population
Very Low (VL)	Only protects against bottom 2% of an avg. threat population

FAIR: Looking Up Vulnerability



		Vulnerability				
	VH	VH	VH	VH	H	M
	H	VH	VH	H	M	L
Tcap	M	VH	H	M	L	VL
	L	H	M	L	VL	VL
	VL	M	L	VL	VL	VL
		VL	L	M	H	VH
		Control Strength				

FAIR: Loss Event Frequency

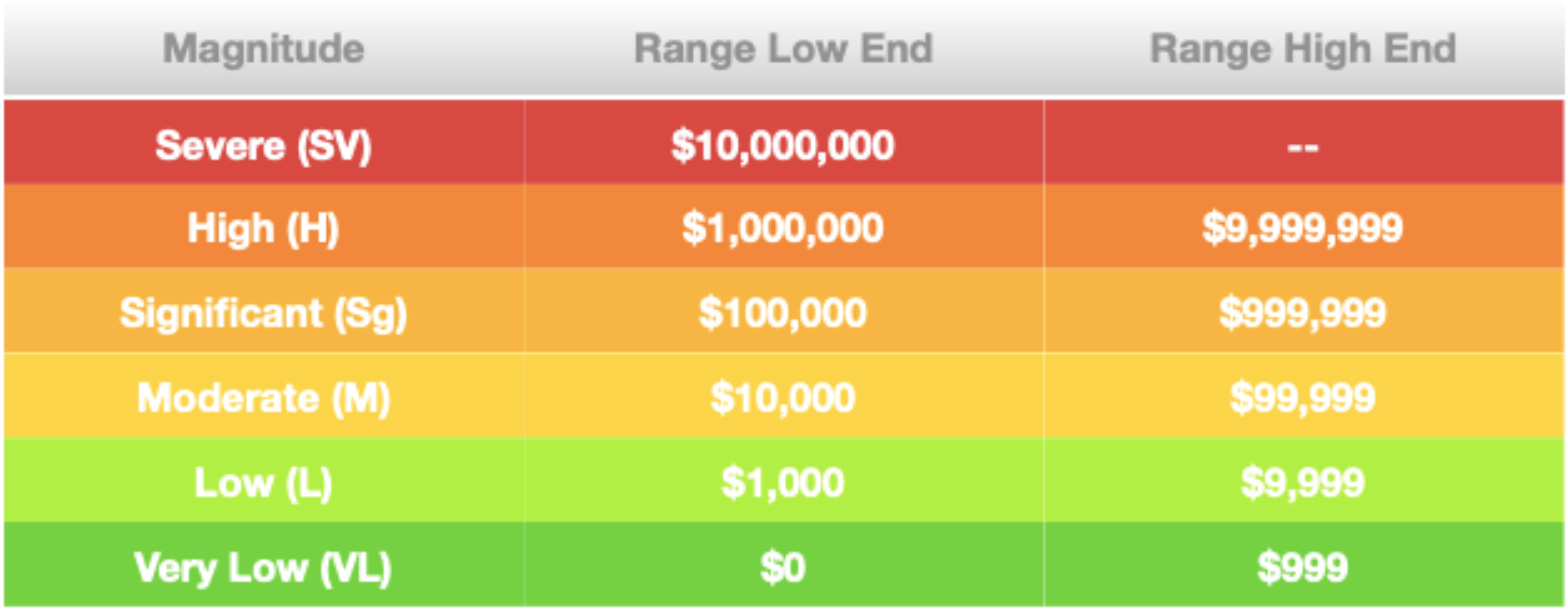


Loss Event Frequency

TEF					
VH	M	H	VH	VH	VH
H	L	M	H	H	H
M	VL	L	M	M	M
L	VL	VL	L	L	L
VL	VL	VL	VL	VL	VL
	VL	L	M	H	VH

Vulnerability

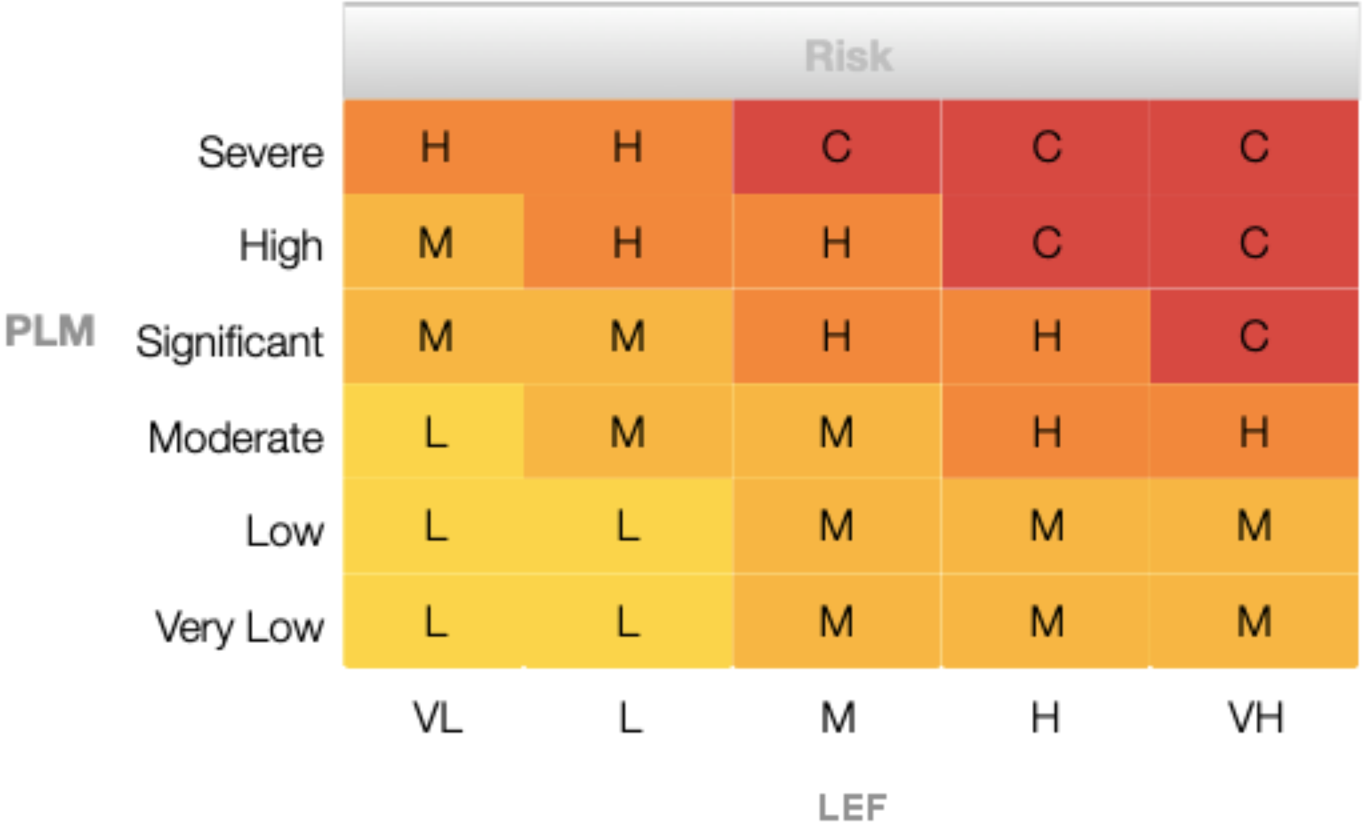
Estimate worst-case loss



Magnitude	Range Low End	Range High End
Severe (SV)	$10,000,000	--
High (H)	$1,000,000	$9,999,999
Significant (Sg)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1,000	$9,999
Very Low (VL)	$0	$999

- Use worst case loss to identify probable loss.

Obtain and Articulate Risk



Risk

PLM	VL	L	M	H	VH
Severe	H	H	C	C	C
High	M	H	H	C	C
Significant	M	M	H	H	C
Moderate	L	M	M	H	H
Low	L	L	M	M	M
Very Low	L	L	M	M	M

LEF

PLM: probable loss magnitude, LEF: loss event frequency

Risk levels: Critical, High, Medium, Low

Colorado State University

Appendix: Octave Allegro: Simple Quantitative Perspective

- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): developed by Software Engineering Institute (SEI) at Carnegie Mellon University in 1999, CERT
- Octave Allegro, 2007
- Can generate a relative risk score
- We will skip, Read yourself if you need to.

OCTAVE Allegro: Improving the Information Security Risk Assessment Process

Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS 559

Risk and Insurance

Based on ILO (International Labour Organization), 2013

CSU Cybersecurity Center
Computer Science Dept

Key questions

- What is risk?
  - What are the different types of risk?
  - What are the sources and consequences of risk?
- How is risk managed?
  - Why do we need insurance?
  - How does insurance work?
  - What is the law of large numbers?
  - What is the J curve in insurance?
- How is probability used in calculating insurance premiums?
- What is asymmetric information?

What is risk?

- Risk is due to an uncertain event which leads to some monetary loss
- Risk is not uncertainty; we know the possible outcomes but not which one will take place
- E.g. Max and Chris are two brothers, who could be either sick or healthy. Thus, there are four possibilities:

Max	Chris
✓	✓
✓	X
X	✓
X	X

- Each outcome has a 25% possibility of occurrence

What is risk?

You do not know:	Sickness	Maternity	Death
Will it happen?	✓		
When will it happen?	✓		✓
What will be the financial Consequences?	✓	✓	

Colorado State University

What is risk?

- We cannot predict which outcome will take place
- However, we can estimate the probability of a risk for a group of people using actuarial techniques

Types of risks: Terminology

- **Covariant risks:** affect large numbers of people at the same time, e.g. epidemics
- **Idiosyncratic risks:** affect a small segment of the population

- **Minor and major risks:**

	Probability	Unit cost	Possible consequences
Minor risk	+++	+	Consultation
Major risk	+	+++	Hospitalization

- **Catastrophic risks:** affect a large segment of the population *and have high unit costs*

Colorado State University

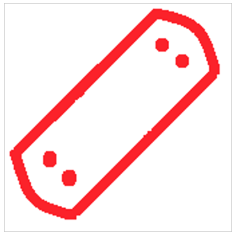
Sources of risk

Natural:	flood, drought
Health:	illness, epidemic
Life-cycle:	birth, old age, death
Social:	crime, war
Economic:	unemployment, financial crisis
Political:	riot, coup d’état
Environment:	pollution, nuclear disaster

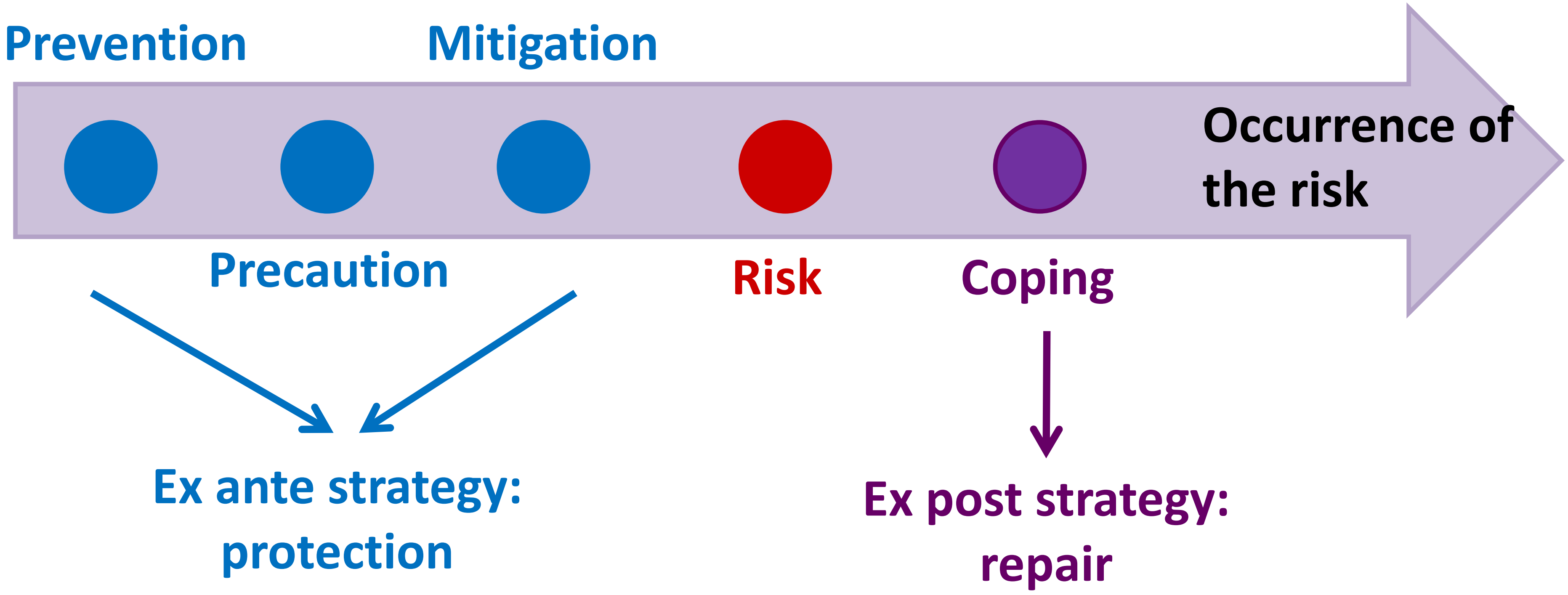
Social security covers health and life-cycle risks, and some economic risks like unemployment (elaborated in Convention No. 102)

Consequences of risk

- Risks have various consequences which could affect the person and the family members
- Thus, risk management is important
- E.g. possible consequences of accidents include financial losses, temporary or permanent disability, death



Risk management strategies



Prevention

Mitigation

Occurrence of the risk

Precaution

Risk

Coping

Ex ante strategy: protection

Ex post strategy: repair

Adapted from R. Holzmann and S. Jørgensen: “Social risk management: A new conceptual framework for social protection and beyond”, in *International Tax and Public Finance* (2001), Vol. 8, No. 4, August, pp. 529-556.

Risk management strategies

Prevention	Precaution	Mitigation	Coping
• aim to reduce the chances of the risk occurring, in advance • are introduced before the risk occurs	• aim to limit exposure to risk • are introduced before the risk occurs	• aim to reduce the potential impact of the risk, in advance • are introduced before the risk occurs	• aim to relieve the impact of the risk after it occurs • are introduced after the risk occurs
e.g. immunization	e.g. settling in areas less prone to floods	e.g. building up assets and savings	e.g. visiting traditional healers to save money, working longer to earn money

Risk management strategies

Choosing a risk management strategy depends on various factors:

- past exposure to risks
- person's capacity for action
- cost-effectiveness and impact of the strategy
- characteristics of the risk e.g. whether the risk can be prevented or mitigated
- context and characteristics of the target group e.g. economic status, size, geographic distribution

Risk management strategies

Ex ante strategies should be favoured over ex post strategies:

- ex ante strategies are more cost-effective and reduce insecurity and vulnerability
- ex post strategies cause greater stress when a risk occurs, especially on women who may have to work more
- households may cope by borrowing money or through child labour, resulting in indebtedness and jeopardizing economic and human development prospects

Need for insurance

Risk management can be done at:

individual level

family level

community level

But not always!

For some risks, individuals, families, communities cannot cope by themselves

There is need for

a broad database

Need for insurance

Risk source	Idiosyncratic	→	Covariant
Natural		landslide	earthquake
Health	illness	epidemic	
	disability		
Life cycle	old age		
	death		
Social	crime	terrorism	war
Economic	unemployment		recession
Political		riots	
Environmental		deforestation	

Informal risk management methods can handle these risks

But break down here

Source: Holzmann & Jørgensen (2000)

Colorado State University

How does insurance work?

A contract!

1. Insured pays a premium

and transfers his financial risk

2. Insurer pays the financial losses suffered by the insured (indemnity) in case of unforeseen events

Colorado State University