Quantitative Security

Colorado State University
Yashwant K Malaiya

CS 559

Risk components & Frameworks

CSU Cybersecurity Center
Computer Science Dept

Today's Menu

- Risk, risk matrices
- Research
- Risk evaluation frameworks
  - RAMCAP
  - FAIR

Risk as a composite measure

Formal definition:

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

  $Risk_i = Likelihood_i \times Impact_i$

- $Likelyhood_i$ may be replaced by $frequency_i$, when it may happen multiple times a year.
- Likelihood can be split in two factors

  $Likelihood_i = P\{\text{A security hole}_l \text{ is exploited}\}.$

  $= P\{\text{hole}_i \text{ present}\}.$

  $P\{\text{exploitation} | \text{hole}_i \text{ present}\}$

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

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/year (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.

ROI

- Businesses often use a term Return on Investment (ROI. it can be defined as

  ROI =

  COUNTERMEASURE_VALUE/COUNTERMEASURE_COST

- Given the following, what is the ROI?
  - ALE_PREVIOUS = $50,000
  - ALE_NOW=$25,000
  - COUNTERMEASURE_COST = $10,000
  - ROI = (50,000-25,000-10,000)/10,000 = 1.5

  (This assumes an annual perspective)

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: 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

Colorado State University

Quick Research

- Mention Quick Research topic by Fri Sept 4.
  - Needed for logistics/scheduling
- Preview of the Term Project
    - What is the current status of technology in this field?
    - What development have taken place recently, say past 2-4 years.
    - What are current products and mature technologies available?
    - Identify 3 organizations (industry, research labs or academic) that seem to have an influential role in advancing the field.
    - Identify the three most important documents as sources of information. These cannot include a textbook (but article in research monograph are OK), and cannot include more than one a promotional blurb from a commercial organization
  - Report (2-3 pages) due Sept 9
  - Slides: (8-12 slides) due Sept 11
    - Post in Canvas Discussions, for instructions
    - Presentations: Sept 15, 17 (15+5 min) in class (videos from distance students)
    - Peer reviews and evaluation

Quantitative Cyber-Security

Colorado State University
Yashwant K Malaiya

CS 559

How to do research
(project/thesis/publication)

CSU Cybersecurity Center
Computer Science Dept

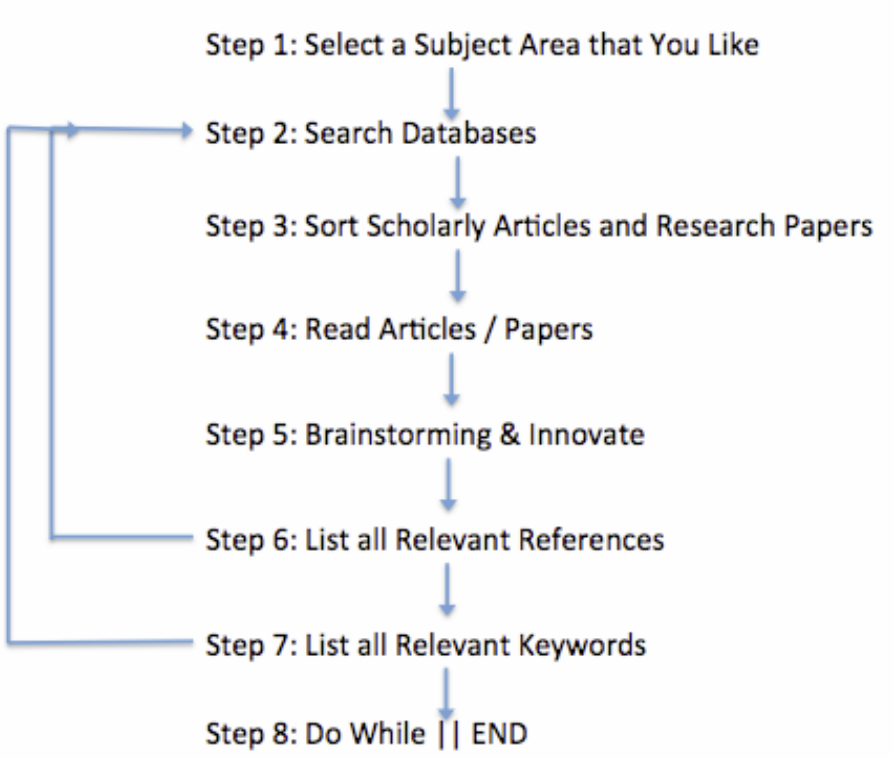
Research Objective

- Become familiar with technical topic of current interest
  - Current state of the art
  - Where the field is going (thus what to expect next)
- Become an expert in the field
  - Should be able to answer important questions
- Original contributions
  - What needs to be done
  - Suggest how it would be addressed
- Present your work
  - Briefly (presentation) and in detail (paper)

Project types

- A thorough survey of a topic, with original insight
- A development of a new scheme
  - or a fresh implementation of an existing scheme
- Modeling and analysis of an existing scheme.
  - If it has not been done/done adequately before
- Development of a hypothesis and evaluating it.
  - Standard statistical methods
- A meaningful combination

Steps for Identifying Sources



How to Start a Research Work in Computer Science:
A Framework For Beginners Somdip Dey
https://xrds.acm.org/article.cfm?aid=2627954

Search Databases

Specific sources: database indexes

- Google Scholar
  - Forward links: Paper X Cited by
  - Backward Links: Paper X cites
- Researcher sites
  - Personal/Group Website
  - DBLP
  - Google Scholar: researcher
- CSU Library etc.

General (*accessible through CSU Library*)

- ACM Digital Library
- IEEEXplore Digital Library
- ScienceDirect etc

Source types

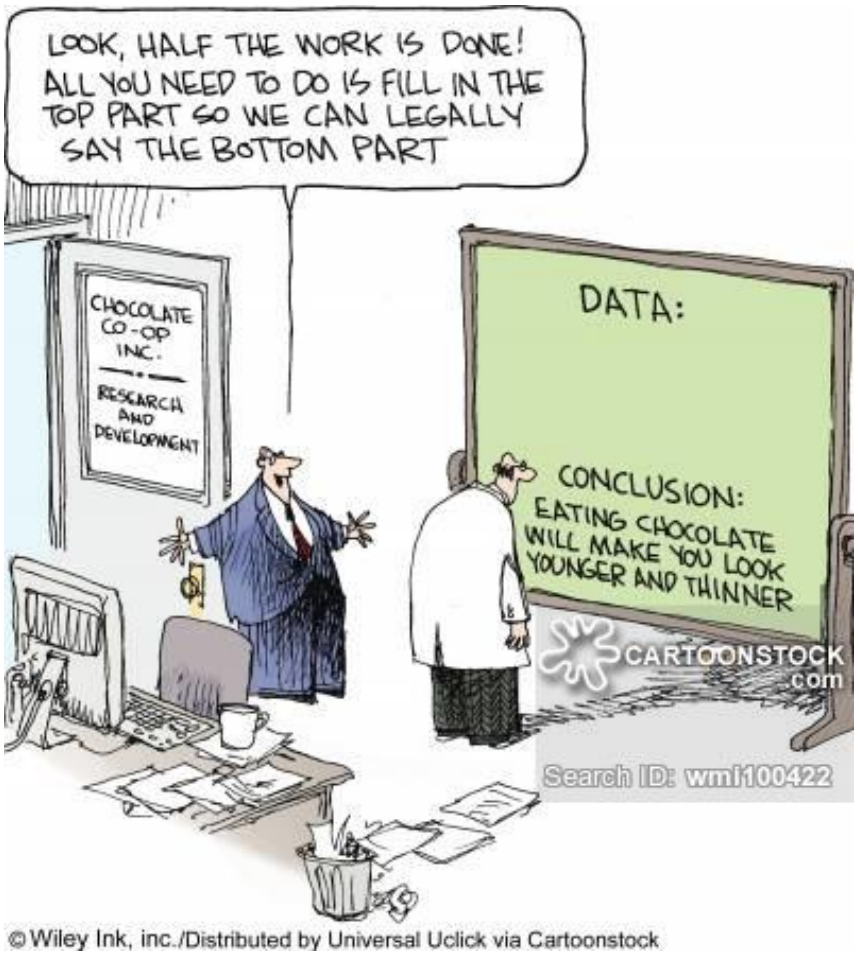
- Journals: published several times a year
  - Rigorously reviewed, long publication delay
  - Journal, Transactions, …
- Conferences: held once a year,
  - Refereed Proceedings: Conference, Symposium, …
  - Workshops: Mildly refereed, often no proceedings
- Research groups
  - Industry, academic, consultants: web site
- Industry publications
  - Magazines, blogs, white papers, product website
  - Annual threat reports
- Books:
  - Textbooks/Trade books: well known things
  - Research monographs/collections

How to Read a Paper: THE THREE-PASS APPROACH

- The first pass: Read
  - the title, abstract, and introduction
  - section and sub-section headings, but ignore everything else
  - the conclusions
- The second pass: Read
  - figures, diagrams, tables and other illustrations
  - mark relevant unread references for further reading
  - Do you need to read it in detail?
- The third pass: Read critically
  - identify and challenge assumption and views
  - Loop up references needed

Keshav, S., How to Read a Paper, ACM SIGCOMM, http://ccr.sigcomm.org/online/files/p83-keshavA.pdf

Avoid Prior Bias



Key Questions

- What problem are you trying to solve?
  - Why is it important to others?
- What recent advances or interesting ideas are there?
  - what have others done?
  - what have others not done yet?
- What have you done (so far)?
  - What is your next step?
  - how does it relate to your goal?
  - why is it important?
- How will you know when …
  - you've made progress?
  - you're done?

William J. Rapaport, How to Write

Proper formatting

- Proper citations: IEEE/ACM format
  - Including authors, title, publication, page numbers/DOI, date.
- Two column IEEE/ACM format
  - Title, name(s) of the author(s), name of the class and professor
  - Abstract
  - Your contribution and what is new
  - Introduction (background & related work, objectives & methods),
  - Assumptions/schemes/models/problem-formulation
  - Comparison/discussion/derivation etc. of the results,
  - Conclusions and suggestions for improvements
  - References.
  - Appendixes (if need)

Must have diagrams and hard technical info (equations/tables/plots/screen-shots etc)

Citing Sources

"IEEE" "ACM" etc:

- These are professional organizations that organize numerous conferences and published journals. They cannot be cited as the "source".
- You must specify the author, title of paper, specific names of conference/journal, associated details, date, page numbers
- A simple URL is not a valid citation
- URL not needed for conference, journal publications. Needed for on-line publications (Organizational reports, Industrial white-papers, News etc)

Omar H., Alhazmi and Yashwant K. Malaiya, "Application of vulnerability discovery models to major operating systems", IEEE Transactions on Reliability, Volume: 57 , Issue: 1, pp. 14-22, March 2008,

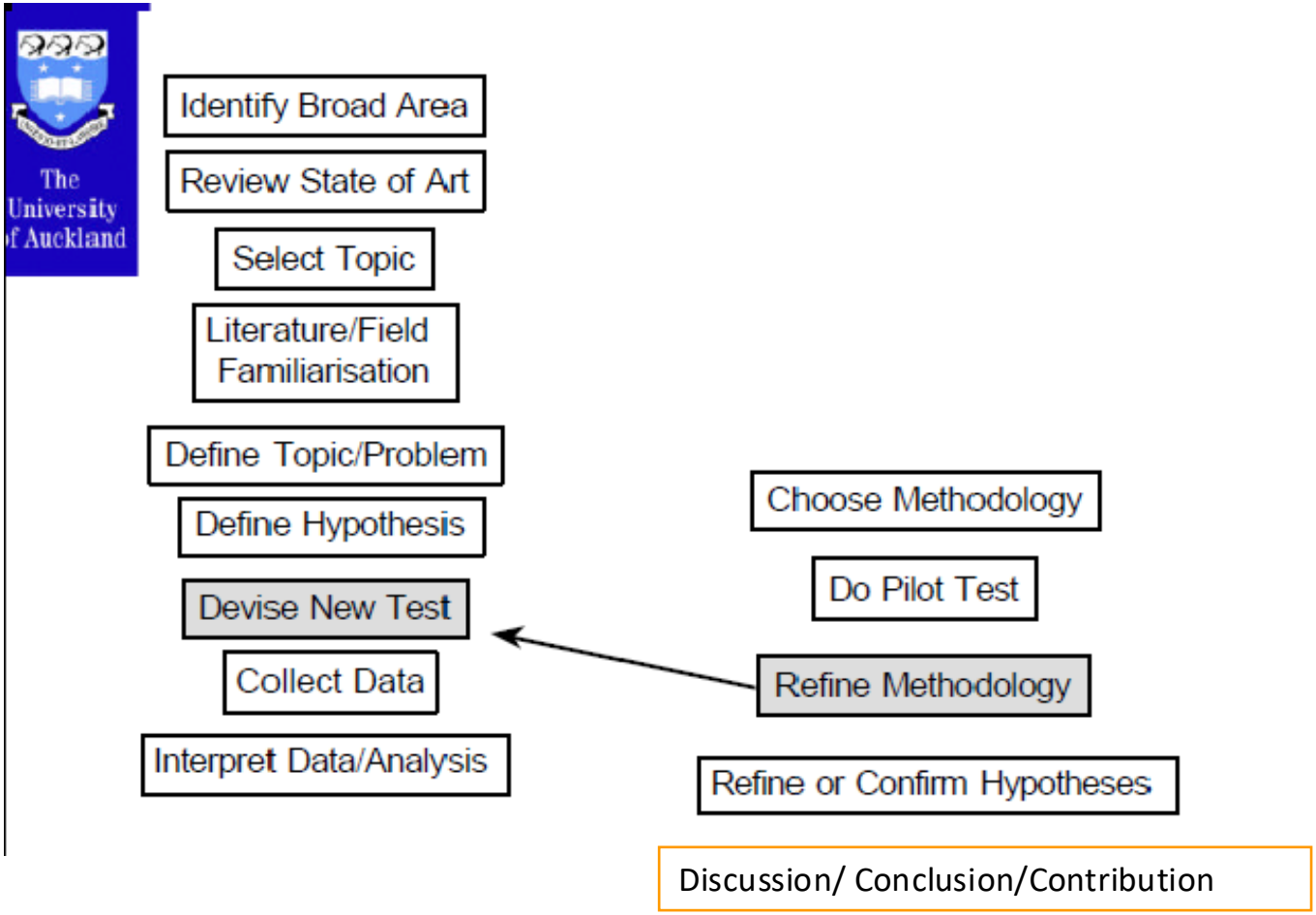
Ambrose Andongabo, Ilir Gashi, "vepRisk - A Web Based Analysis Tool for Public Security Data", 13th European Dependable Computing Conference (EDCC) 2017, pp. 135-138, 2017.

Evaluation

Similar to paper review for conferences/journals

- Significance and originality
- Thoroughness of research
- Depth of understanding displayed
- Presentation
- Final report is submitted through TurnItIn using Canvas
  - Checks for overlap with other documents (plagiarism)
  - Some overlap OK
  - Cite sources of definitions, ideas, data, figures etc.
  - Any text copied and pasted must be enclosed in quotes and cited
    - Exception: references (cite only those you have seen)
  - Also checked manually for genAI

Typical Original Research Process



Citing Sources

"IEEE" "ACM" etc:

- These are professional organizations that organize numerous conferences and published journals. They cannot be cited as the "source".
- You must specify the author, title of paper, specific names of conference/journal, associated details, date, page numbers
- A simple URL is not a valid citation
- URL not needed for conference, journal publications. Needed for on-line publications (Organizational reports, Industrial white-papers, News etc)

Omar H., Alhazmi and Yashwant K. Malaiya, "Application of vulnerability discovery models to major operating systems", IEEE Transactions on Reliability, Volume: 57 , Issue: 1, pp. 14-22, March 2008,

Ambrose Andongabo, Ilir Gashi, "vepRisk - A Web Based Analysis Tool for Public Security Data", 13th European Dependable Computing Conference (EDCC) 2017, pp. 135-138, 2017.

You must include

- Title, your name, class, year, professor's name
- Abstract: What does it include and why is it important
- Background: Other existing work and background ideas
- Technical discussion: detailed discussion of findings with non-text material (charts, plots, tables. algorithms etc)
- Discussion & Summary
- References

You Must Do Research

Not enough:

- Summary of a couple of papers
- Summary of work of a single research group
- Rephrasing of existing surveys

You must know (and should be able to answer related questions):

- Current state of the art
- Alternative approaches and how they can be evaluated
- Technology trend
- Find data describing the technology
- Existing issues and challenges

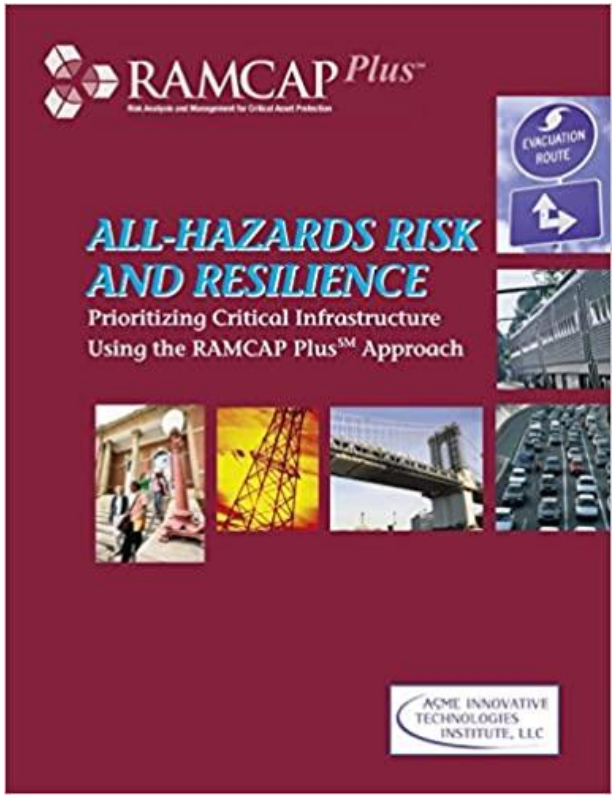
Risk Evaluation

- These frameworks are for general purpose use, including cyber security.
- Evaluating risk qualitatively when exact quantitative measurements are not available.

Risk Evaluation Frameworks

- Attempts to list what is known and estimate the risk
- Qualitative -> Semi-Quantitative -> Quant. estimates
- Examples
  - **RAMCAP**
  - **FAIR**
  - OCTAVE
  - *How to Measure Anything* in Cybersecurity Risk, 2016 (Hubbard-book)
  - Approach specific terminology and procedures
- *People are expected to hire consultants or take courses that include details of the methodology. Some related computational tables or tools are available.*

RAMCAP Framework



- 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 Framework

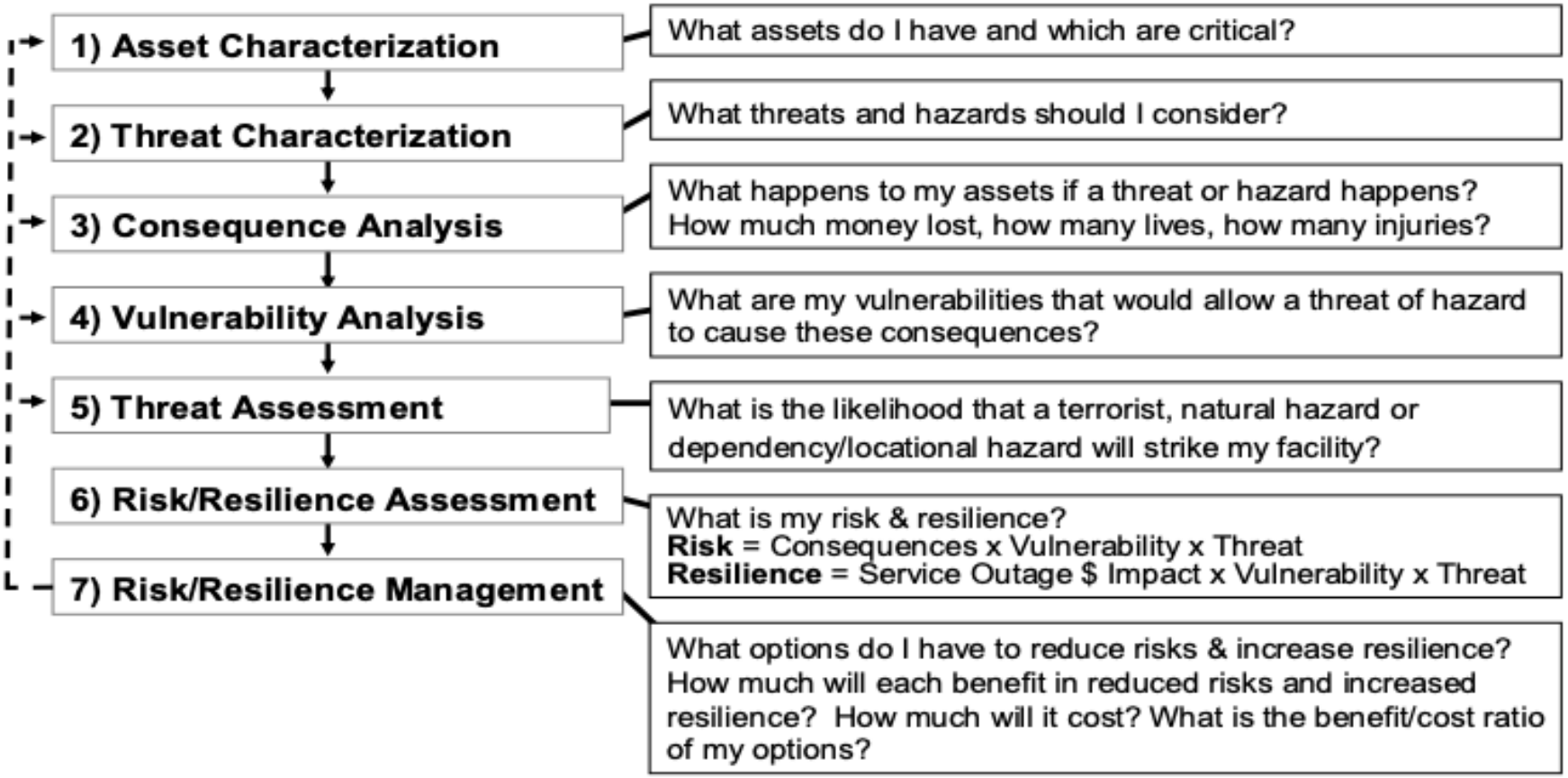
- Following Sept 11, 2001 attack, ASME (formerly known as the American Society of Mechanical Engineers) convened more than one hundred industry leaders, at the request of the White House, to define and prioritize the requirements for protecting USA's critical infrastructure.
- Recommendation: a risk 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

RAMCAP: Risk and Resilience Defined

- Risk = Threat x Vulnerability x Consequence*
  - Note terminology is from classic risk literature
  - Vulnerability: Prob of internal weakness
  - Threat: Prob of the weakness getting exploited
- 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. *Defined negatively in RAMCAP*
  - $Resilience_{Owner}$ = Lost Net Revenue x Vulnerability x Threat
  - $Resilience_{Community}$ = Lost Community Economic Activity x Vulnerability x Threat

The 7-step RAMCAP Plus Process



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

- **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

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*

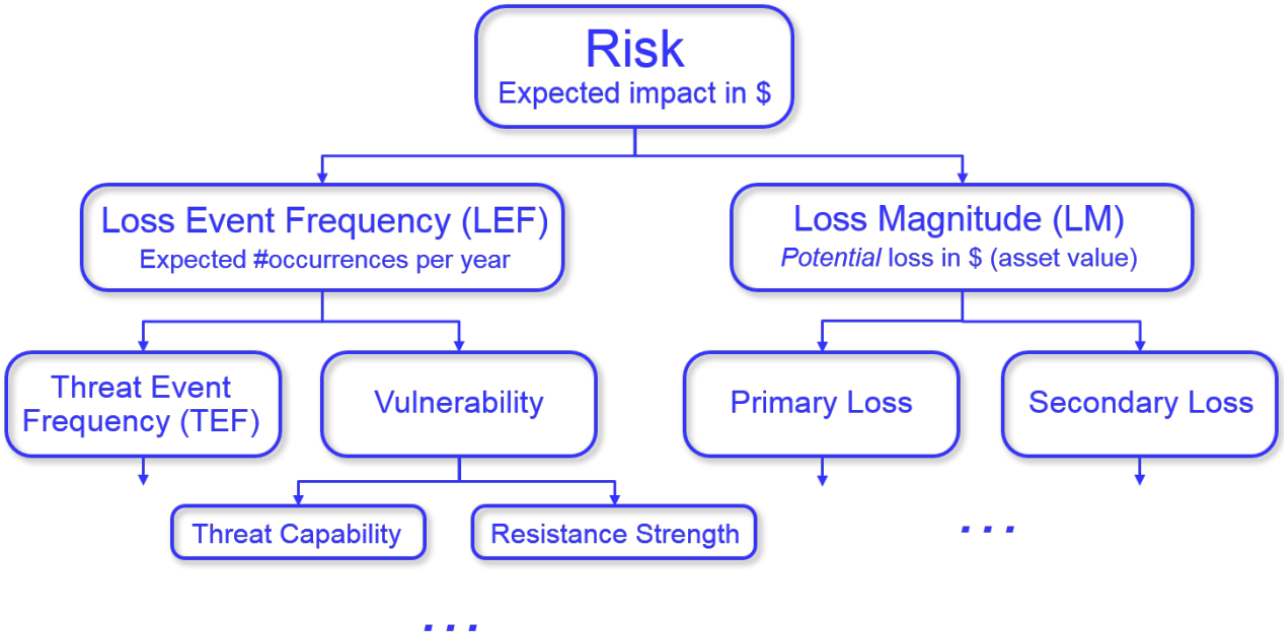
- Distortions Due to Use of Arithmetic Averages on Logarithmic Scales
- Improper granularity may be used
- Product of Expected Values Not Equal to Expected Value of Product
- Priority Ranking May Not Support Effective Resource Allocation
- "Threat" Is Not Necessarily Well Defined
- "Vulnerability" Can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

Observation: Many factors cannot be evaluated exactly. The challenge is to make analysis as accurate as possible using available information based on prior studies.

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.



An Introduction to FAIR, Jack A. Jones, 2005

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 of Control 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, Jack A. Jones, 2005

FAIR Framework: 4 Stages

Stage 1: Identify Scenario Components

- *Identify asset at risk:*
- *Identify the threat community: external/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

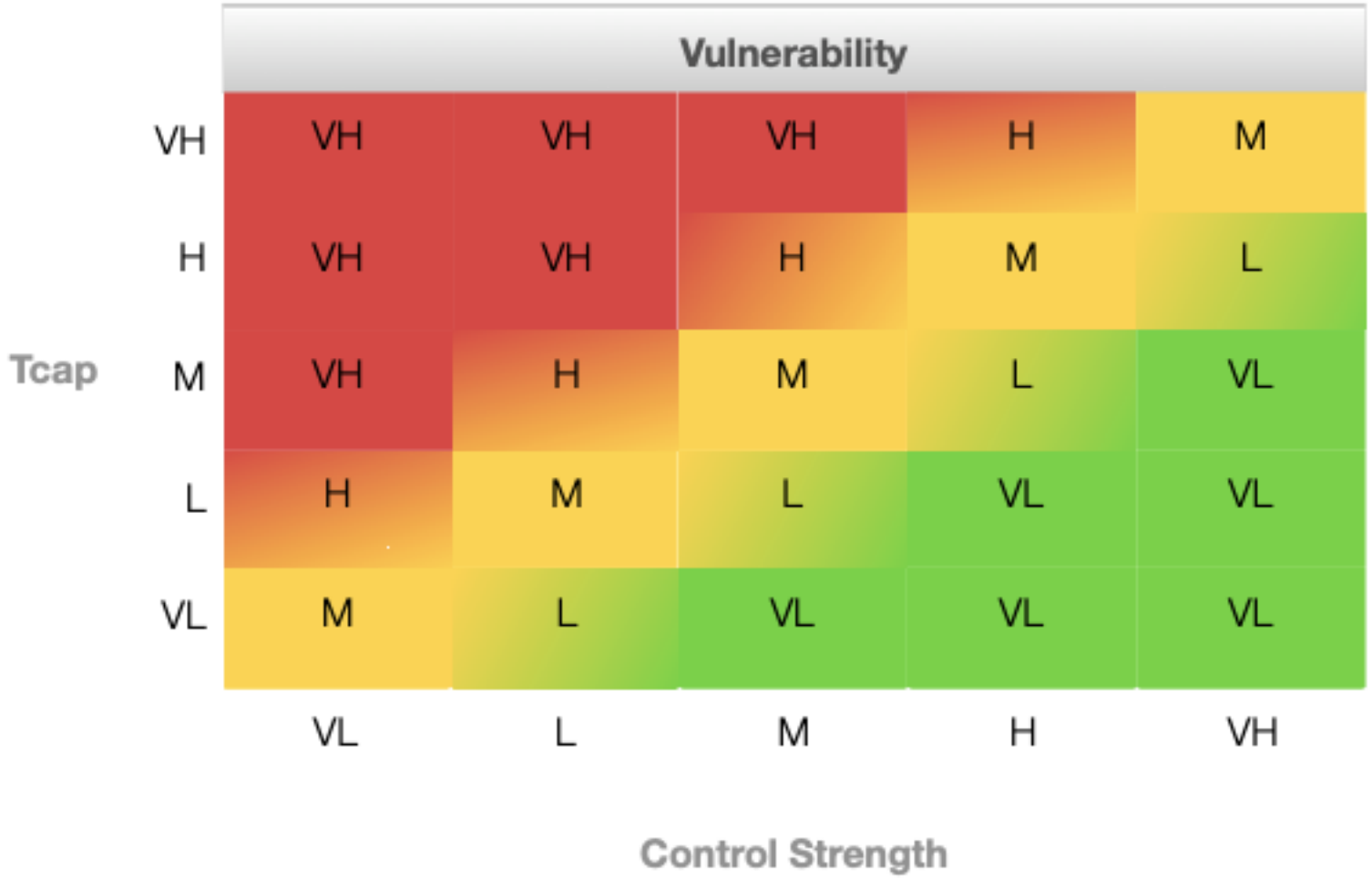
Tcap rating	Description
Very High (VH)	Top 2% when compared against the overall threat population
High (H)	Top 16% when compared against the overall threat population
Moderate (M)	Average skill and resources (between bottom 16% and top 16%)
Low (L)	Bottom 16% when compared against the overall threat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

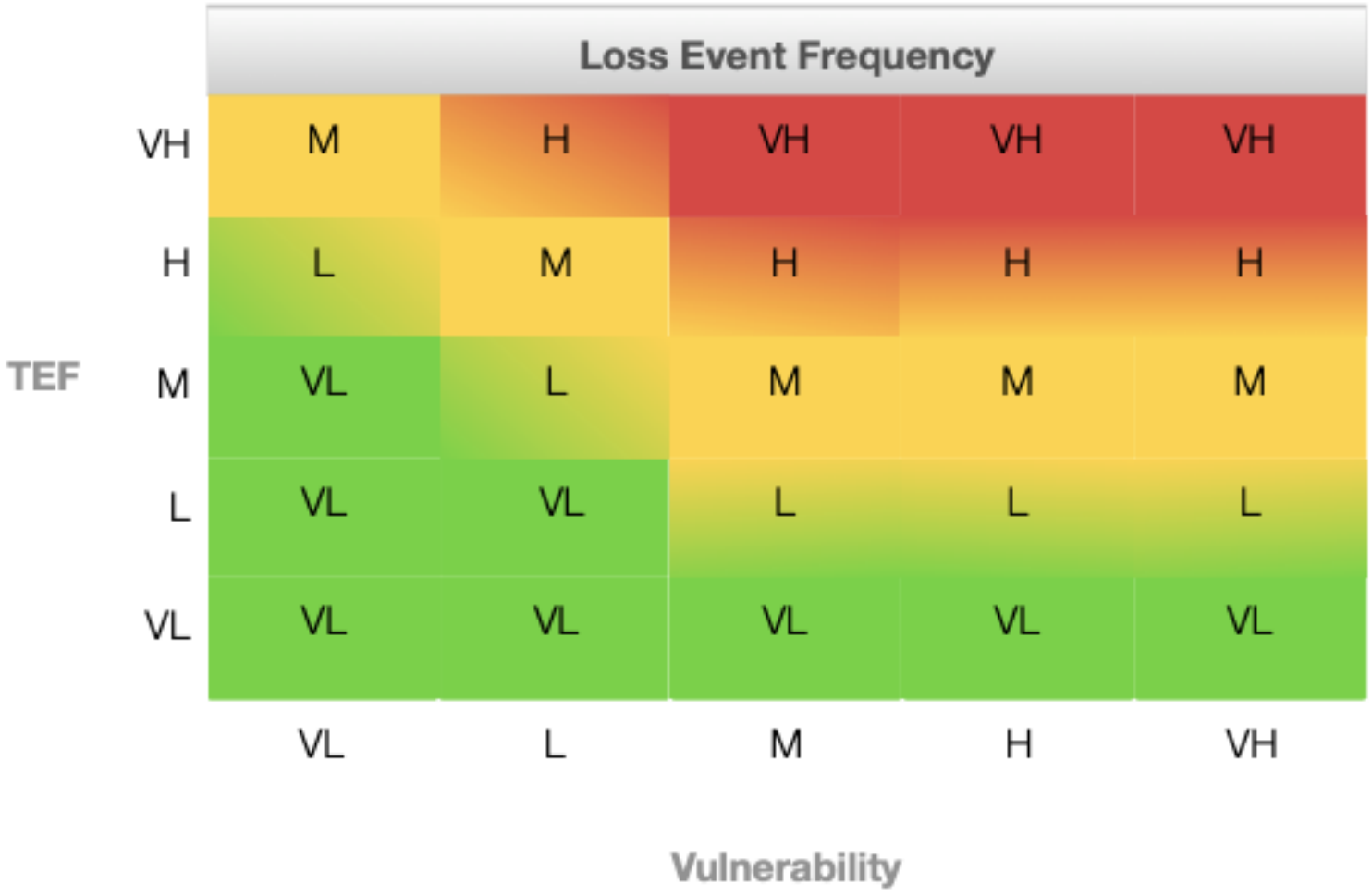
FAIR: Looking Up Vulnerability



Vulnerability level = f(Threat capability level, Control Strength level)

Colorado State University

FAIR: Loss Event Frequency



Loss Event Frequency level= f(Vulnerability level, Threat Event Frequency)

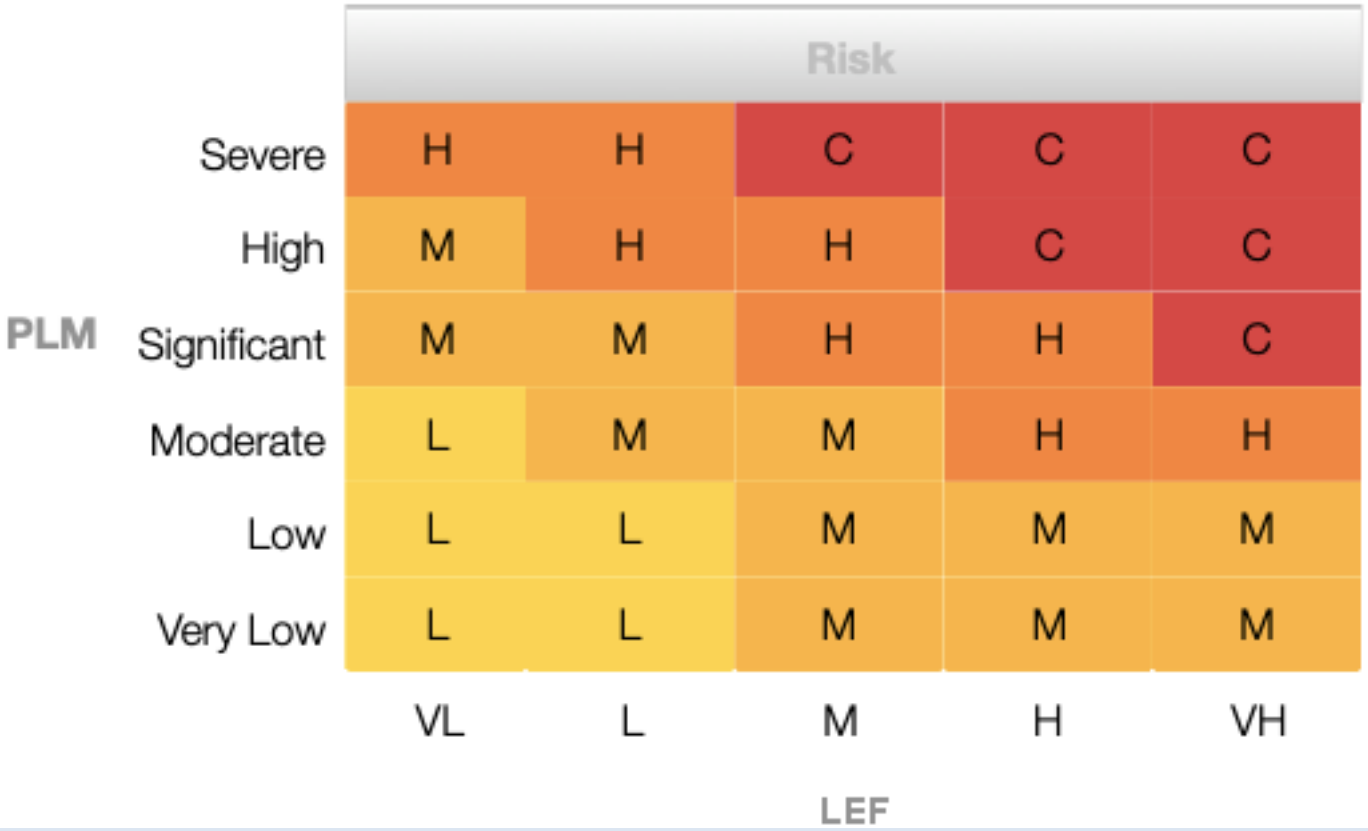
Colorado State University

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 magnitude (PLM).

Obtain and Articulate Risk



Risk= f(PLM: probable loss magnitude, LEF: loss event frequency)

Risk levels: Critical, High, Medium, Low

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

NIST Cybersecurity Framework (CSF)

Not a quantitative risk evaluation framework, but a set of approaches for cybersecurity. The framework is organized around 6 *Core Functions* (2.0 release 2024):

List based approach. Each *function* below is divided into 3 to 5 *categories,* further divided into 3-6 sub*categories.*

NIST Cybersecurity Framework (CSF)

List based approach. Each *function* below is divided into 3 to 5 *categories,* further divided into 3-6 sub*categories.*

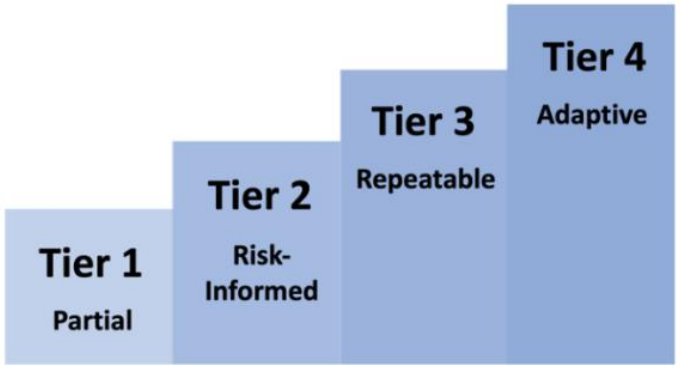
Proactive:

- **Govern:** Establish the organization's cybersecurity strategy, policies, roles, and risk management expectations.
- **Identify:** Discover, inventory, and understand the organization's physical and digital assets, vulnerabilities, and business risks.
- **Protect:** Implement safeguards—such as identity management and awareness training—to prevent or limit a cyber event.

Reactive:

- **Detect:** Maintain continuous monitoring capabilities to find and flag anomalous activity and security events quickly.
- **Respond:** Execute rapid containment, analysis, mitigation, and communication strategies once a security incident is detected.
- **Recover:** Restore operational capabilities, systems, or services that were impaired during a breach.

NIST CSF Tiers



Maturity Tier	Description
Tier 1: Initial	Processes and controls are ad-hoc, informal
Tier 2: Developing	Processes and controls are managed and documented
Tier 3: Defined	Processes and controls are standardized
Tier 4: Advanced	Processes and controls are continuously assessed for improvements

CSF Tiers for cybersecurity risk governance and management