Quantitative Security

Colorado State University
Yashwant K Malaiya

CS 559
Risk and Insurance

CSU Cybersecurity Center
Computer Science Dept

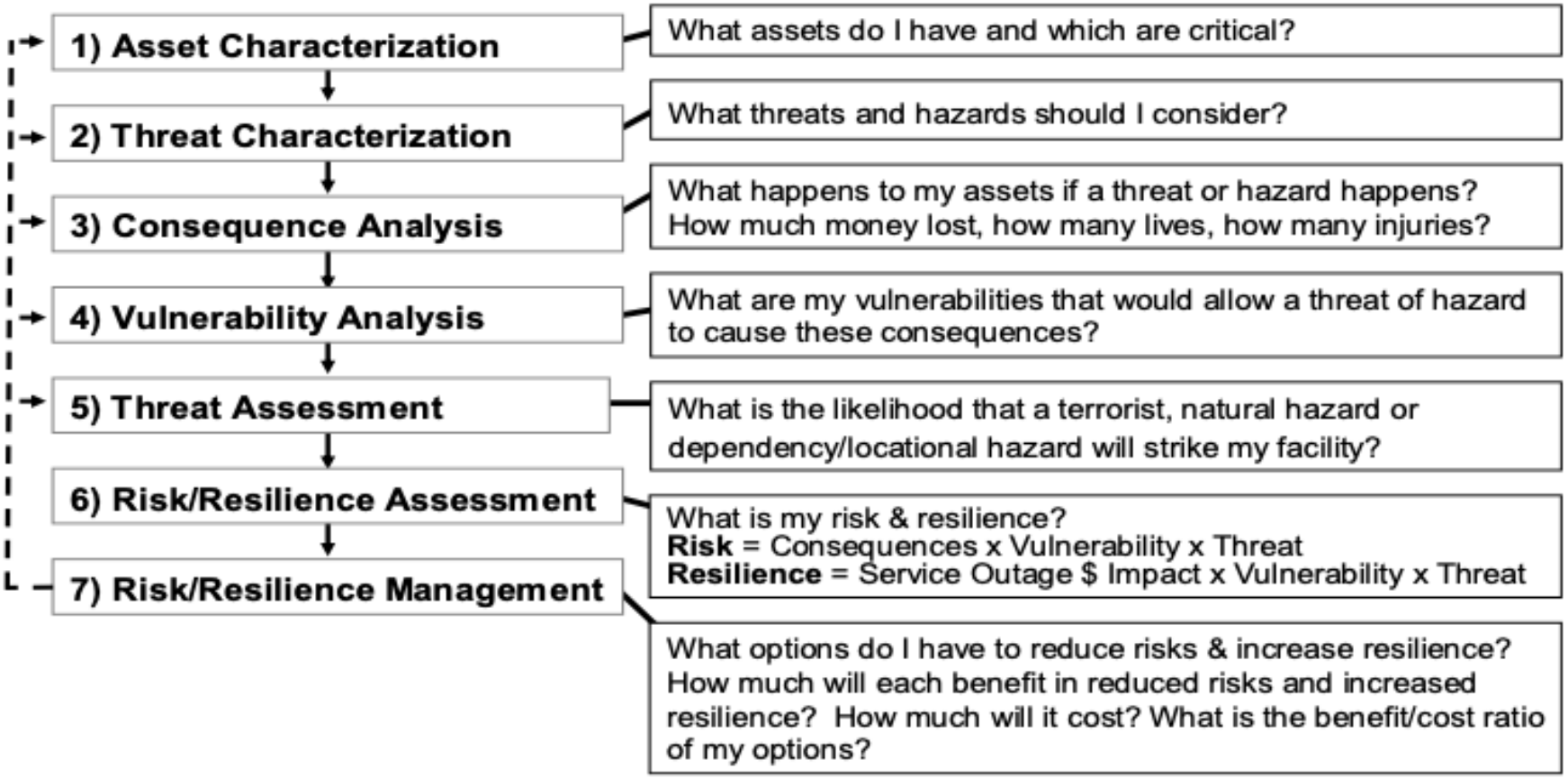
Today

- Risk Frameworks (continued)
- Insurance: Key ideas

Risk Evaluation Frameworks

- Attempts to list what is known and estimate the risk
- Qualitative -> Semi-Quantitative -> Quant. estimates
- Examples
  - **RAMCAP**
  - **FAIR**
  - OCTAVE
  - 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.*

The 7-step RAMCAP Plus Process



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

Colorado State University

The 7 Steps

Lists

- **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

Numerical data:

- **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

Numerical data, formulas:

- 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*

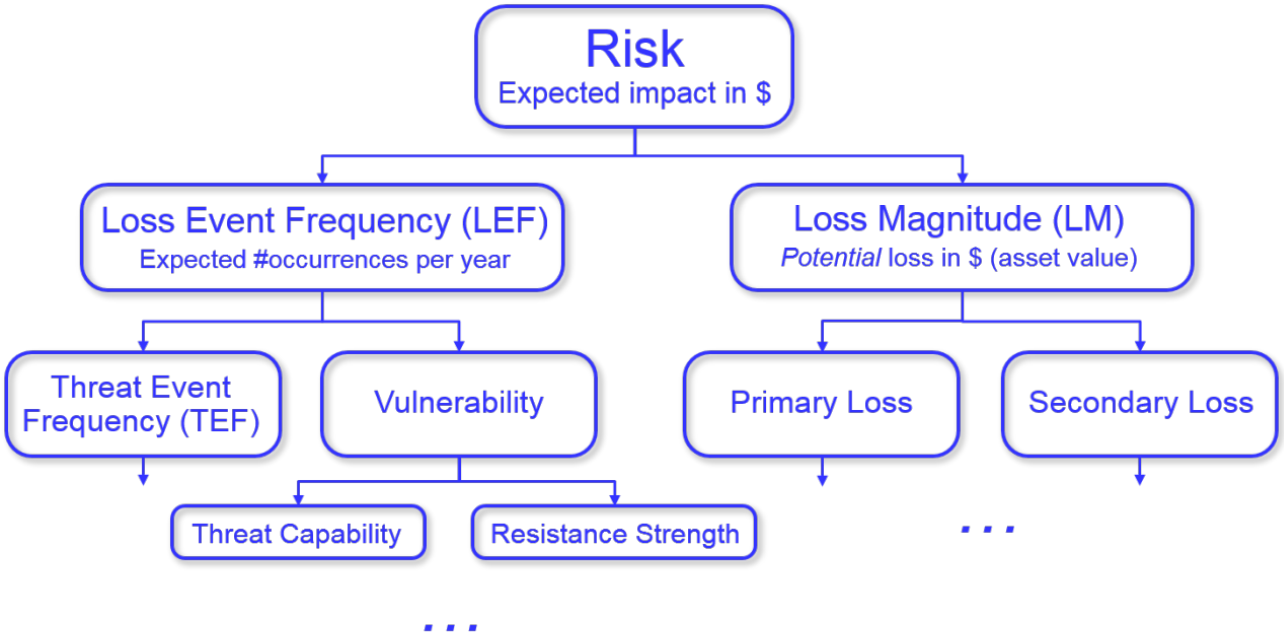
- Distortions Due to Use of Arithmetic Averages on Logarithmic Scales
- Improper granularity may be used
- Product of Expected Values Not Equal to Expected Value of Product
- Priority Ranking May Not Support Effective Resource Allocation
- "Threat" Is Not Necessarily Well Defined
- "Vulnerability" Can 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: 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

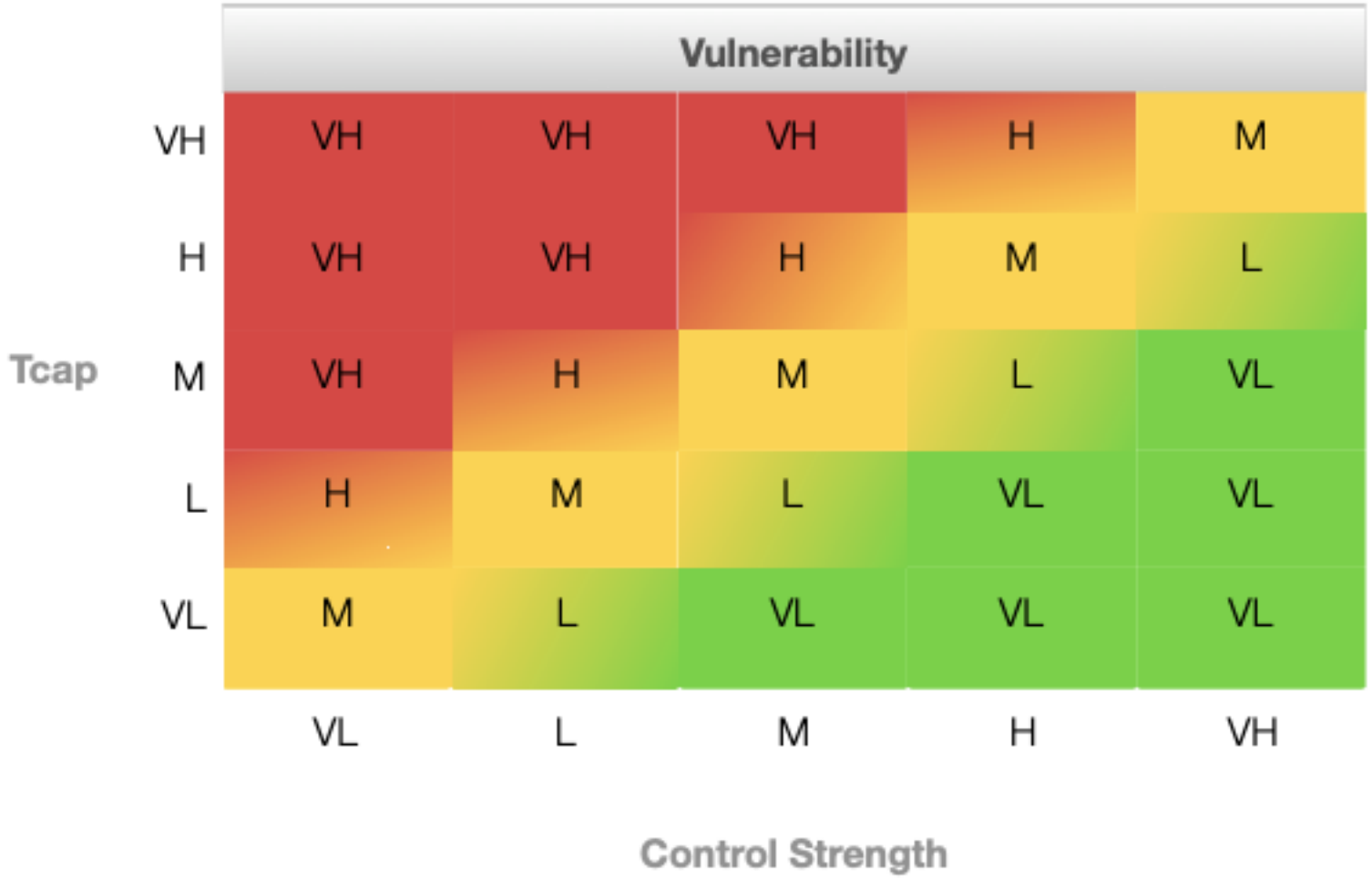
Tcap rating	Description
Very High (VH)	Top 2% when compared against the overall threat population
High (H)	Top 16% when compared against the overall threat population
Moderate (M)	Average skill and resources (between bottom 16% and top 16%)
Low (L)	Bottom 16% when compared against the overall threat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

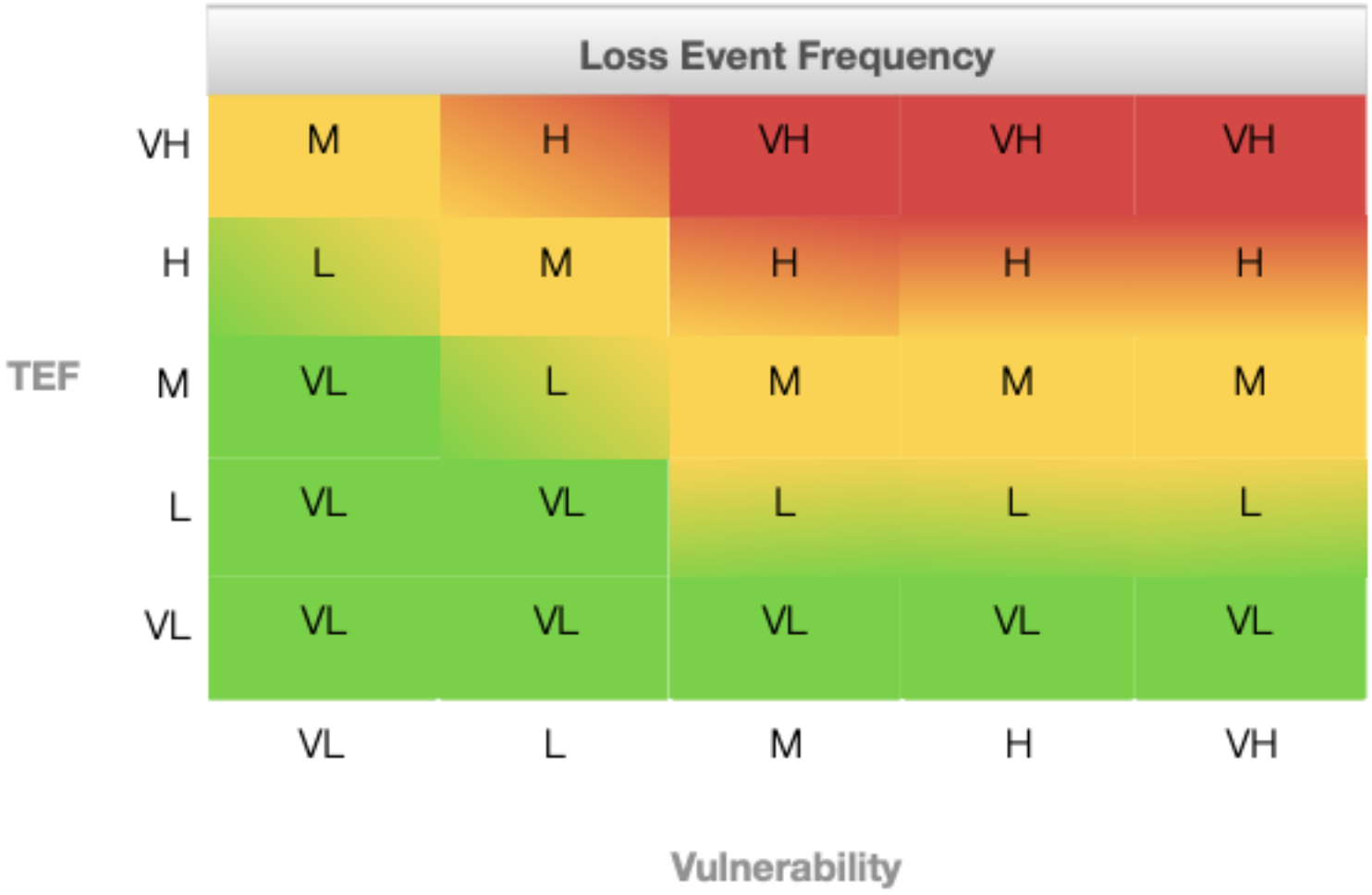
FAIR: Looking Up Vulnerability



Vulnerability 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)

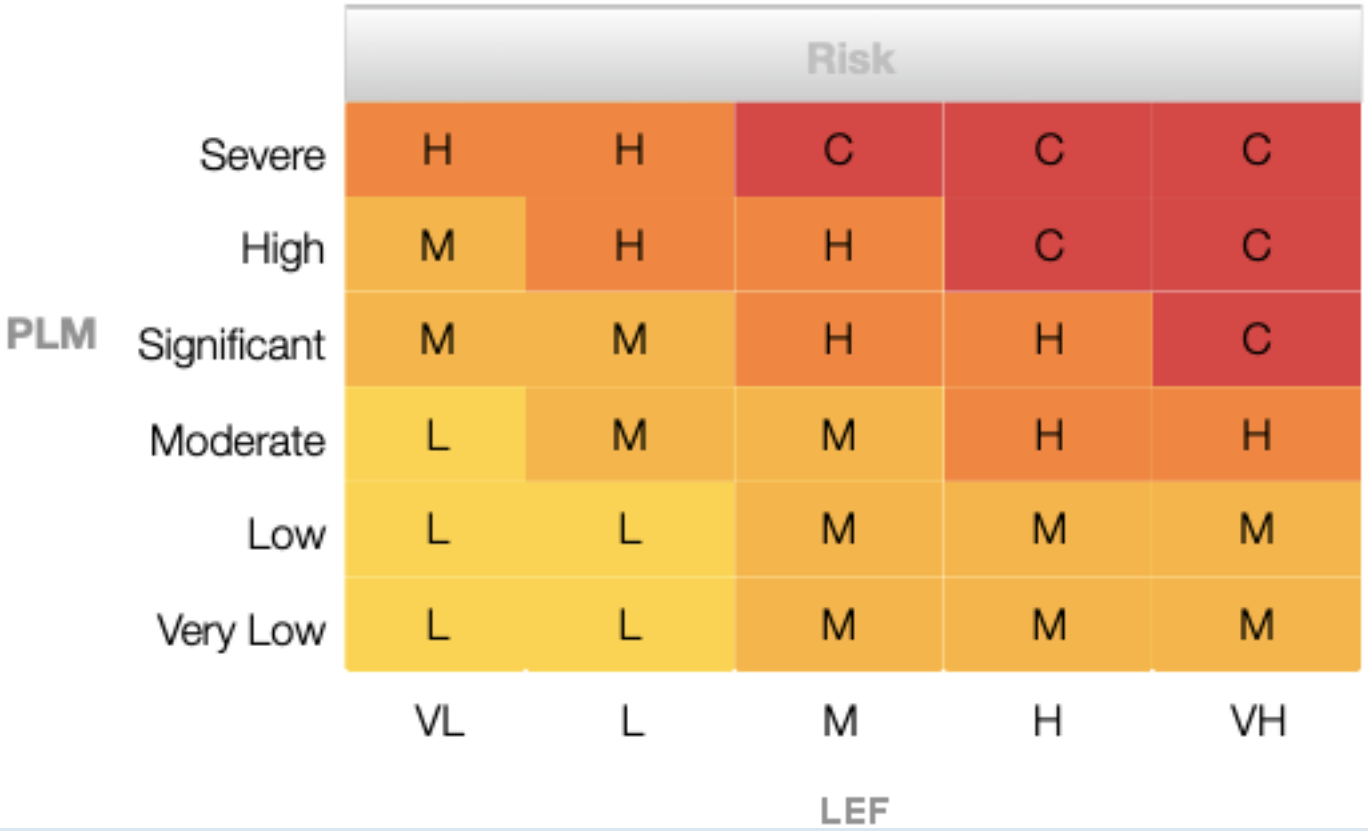
Colorado State University

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

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?

Most examples here are from health and life insurance

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?	✓	✓	

✓ What is uncertain

Colorado State University

Types of risk events: Terminology

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

- **Minor** (low cost) **and major** (high cost) **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, e.g. a major earthquake*

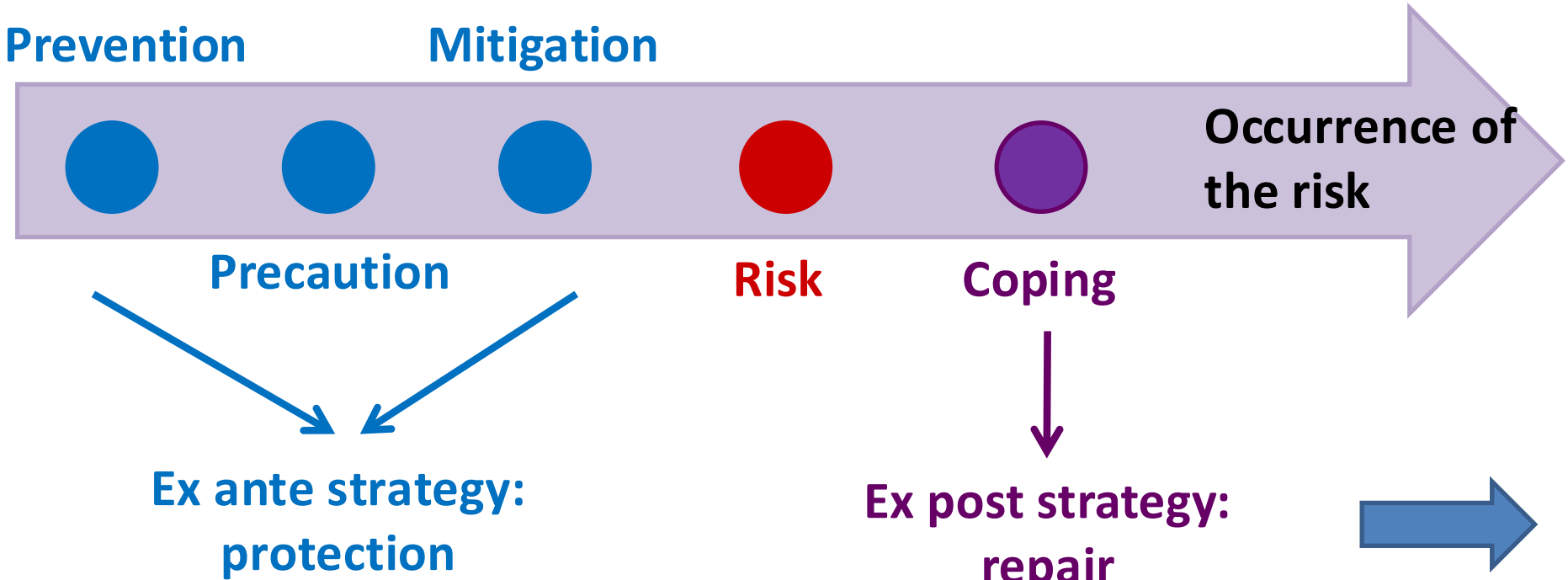
Sources of risk events

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

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

Last three can induce cyber attacks

Risk management strategies



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 Health related examples

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

Colorado State University

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

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

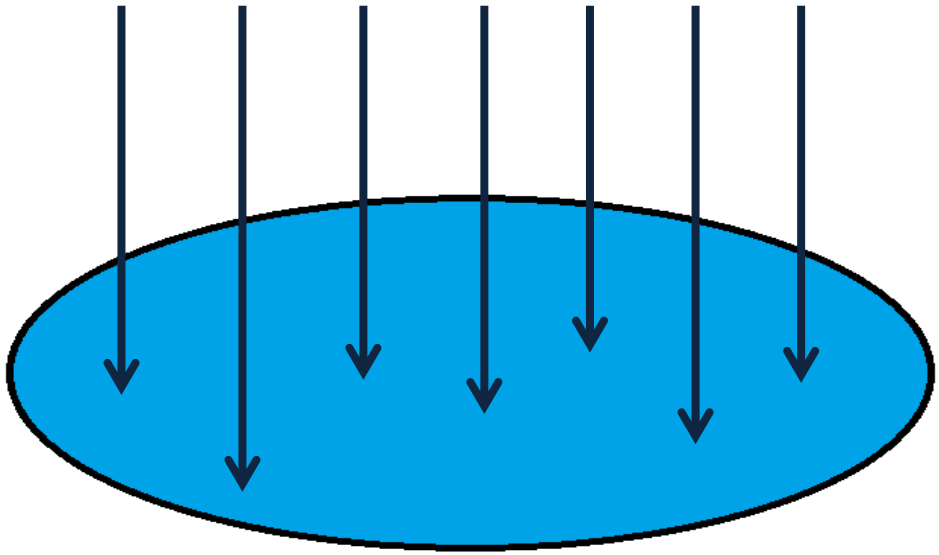
Colorado State University

How does insurance work?

- Illness is unpredictable and need for treatment is uncertain, so individuals cannot predict their future health care expenditure
- Based on historical information, insurance providers can predict the probability of a risk for a large group of insured people and estimate the average cost of the risk
- True for security breach risks except ..

How does insurance work?

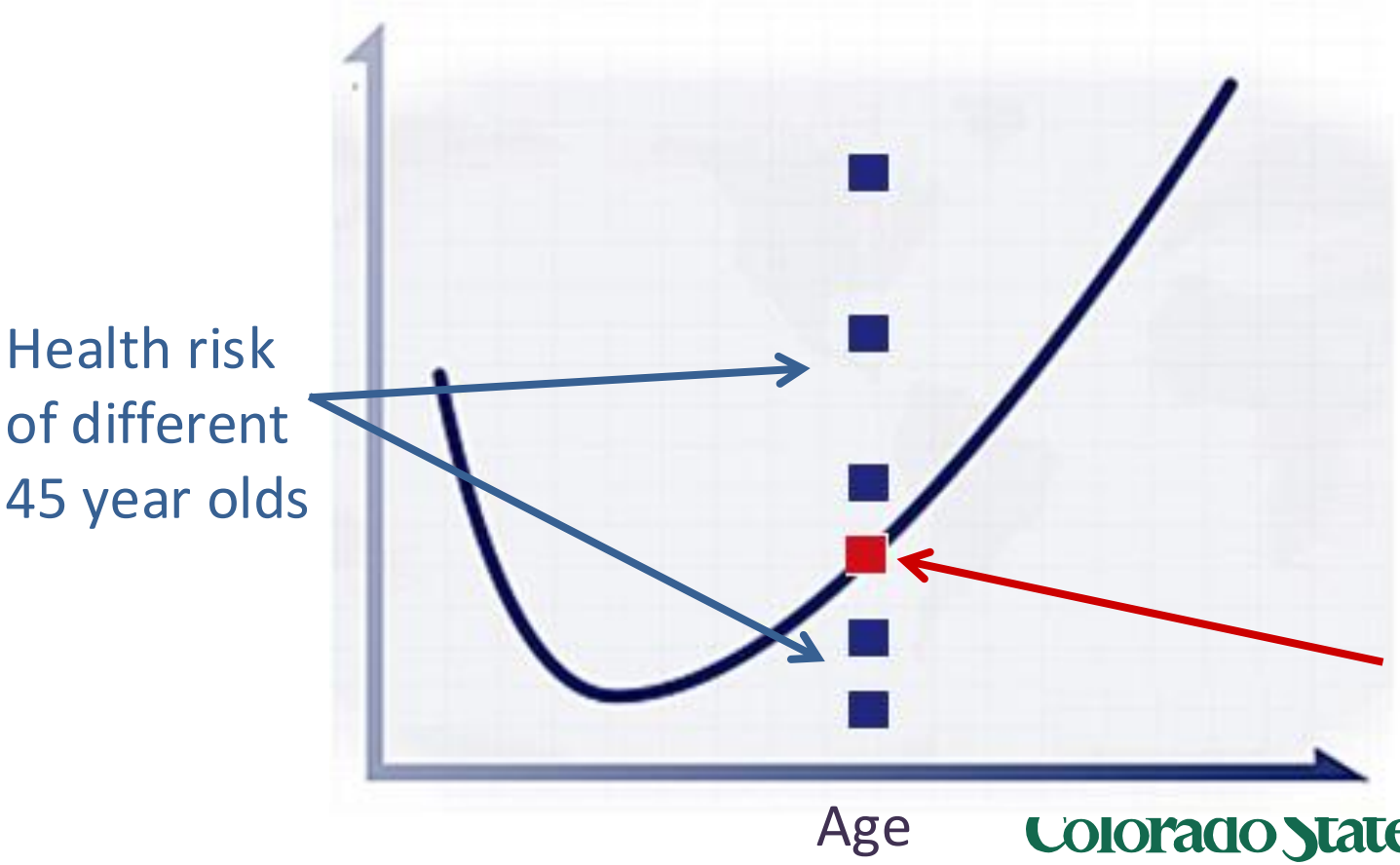
- Insurance takes all the risks in a group and puts them into a pool



- Not all insured persons claim their benefits at the same time
- Contributions paid by all insured members are used to compensate for the financial consequences of the few persons who experience the risk

Law of large numbers

Based on the "Law of large numbers", it translates each individual risk into an average of all risks

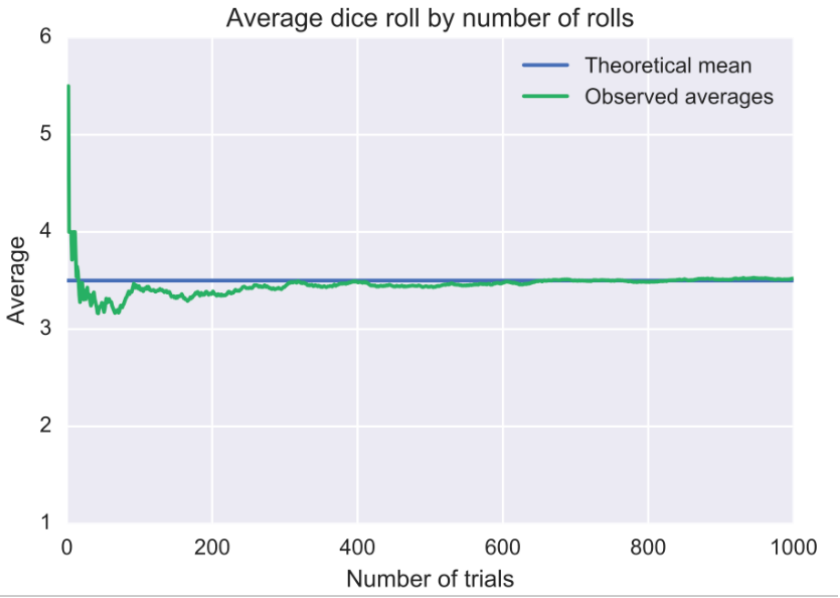


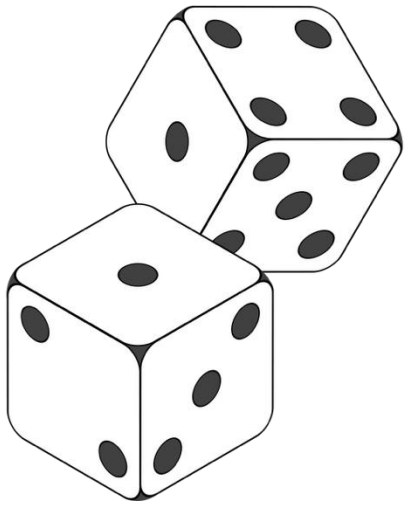
Colorado State University

Law of large numbers

The **law of large numbers**: the average of the results obtained from a large number of trials should be close to the expected value and will tend to become closer to the expected value as more trials are performed.

- *Sample mean* vs *population mean*.





- When insurance is provided to a very large group of people, the expected losses are similar to the average of all individual losses.

Calculating insurance premiums

In Insurance that is *actuarially fair*, the premium is equal to expected claims (ignores overheads/company profit).

Example 1: Kate was born with a rare disease and has a 40% chance of relapse in a year. If relapse occurs, she has to visit a doctor for consultation once every 3 months. Each consultation costs 30$. Calculate the fair insurance premium.

Premium = probability of illness in a year x average no. of utilization of services per year x unit cost of each utilization

= 0.4 x 4 x 30$

= 48$

40% = 40/100 = 0.4

Actuaries analyze the financial costs of risk and uncertainty.

Calculating insurance premiums

Example 2 (cont.): Further, in the consultation the doctor may either prescribe medication or recommend that she take laboratory tests. Probability of prescription is 80% while that of tests is 20%. Cost of medication is 50$ and cost of tests is 150$. Calculate the fair health insurance premium.

Premium = probability of illness in a year x average no. of utilization of services per year x unit cost of each utilization

= 0.4 x 4 x [30$ + (0.8 x 50$) + (0.2 x 150$)]

= 0.4 x 4 x [30$ + 40$ + 30$]

= 0.4 x 4 x 100$ = 160$

Loss Ratio

- The loss **ratio is** the ratio of incurred losses and loss adjustment expenses to premiums earned.

$$Loss\ Ratio = \frac{incurred\ losses + loss\ adjustment\ expenses}{premiums\ earned}$$

- *Example:* A company paid $133.6 million in losses and $14 million in loss-adjustment expenses. Premiums earned were $205 million.

$$Loss\ Ratio = \frac{133.6 + 14}{205} = 0.72$$

- The loss ratio is often in the 65 percent to 75 percent range. Thus the insured pool with get back about 65 to75% of the premiums paid. Affordable Care Act (ObamaCare)requires it to be minimum 80% (85% for large groups).

Principles of risk Management and insurance, Rejda, McNamara, 2017

Ranges

- High Ratio (>85%–100%): Signals financial distress; the insurance company pays out more in claims than it brings in via core coverage revenue.
- Very Low Ratio (<40%): May indicate overly restrictive underwriting or excessively high pricing, which can trigger regulatory scrutiny or customer loss
- Optimal Range (50%–70%): Indicates healthy underwriting profitability, leaving enough room for operational expenses and profit.

Typical Loss Ratios

Type	Typical range	Context
Auto	65-80%	High claim frequency
Health	80-88%	Regulated (ACA requires 80-85%)
Property	55-65%	Prone to severe weather spikes, catastrophic losses

First-party and Third-party Insurance

First-party insurance

- First-party: losses to the insured organization
- Loss or damage to digital assets
- Business interruption
- Cyber exhortation
- Customer notification expenses
- Reputational damage
- Theft of money or digital assets

Adapted from the Association of British Insurers

Third-party insurance

- Third-party: losses due to claims made by others (customers, etc.)
- Investigative or defensive costs associated with security and privacy breaches
- Multi-media liability (e.g., breach of privacy or negligence in publication in electronic or print media)
- Loss of third-party data

What is Reinsurance?

- An arrangement whereby **an insurer transfers all or part of a risk to a reinsurance company to provide protection against the risk of the primary insurer**.

- Cyber reinsurance is specifically designed for primary cyber insurance companies, offering them protection against large or catastrophic cyber events that could impact their portfolios

Asymmetric information

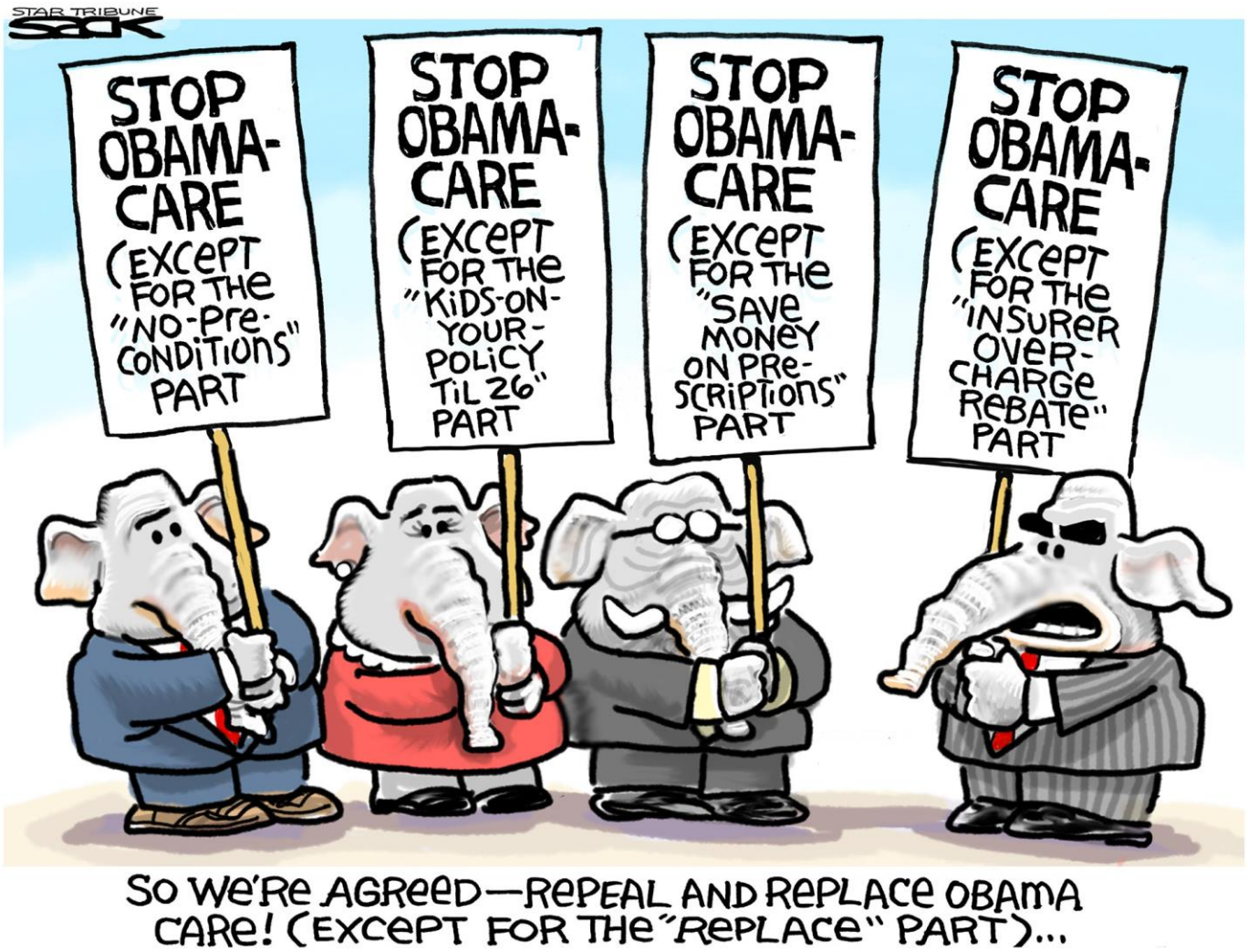
Adverse selection

- The insured person conceals information that places them in a high-risk bracket
  - Thus, average risk of the insured group increases and premium rises
  - May cause low-risk people to leave, high-risk people are left in the group
  - E.g. Bob must undergo a surgery within the next 10 months and joins a health insurance scheme, knowing that the operation will be covered when the waiting period is over. (*preexisting condition*)

Moral hazard

- The insured person takes risks and is careless about their safety, knowing that they are protected from financial losses
  - E.g. Jenny has a good insurance policy and goes to see her general practitioner, allergist, gynaecologist and dermatologist at least once every month

Replacing Obamacare



Colorado State University

Asymmetric information

Ways to minimize adverse selection and moral hazard

- establish mandatory insurance, so that high-risk and low-risk people are members of the risk pool
- exclude predictable events such as planned surgeries from the benefit package
- implement co-payments and limitations, e.g. maximum number of days of hospitalization, health expenditure reimbursement up to a maximum level
- establish long waiting periods
- put in place control mechanisms like pre-authorization of high-cost planned surgeries

Appendix

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.*

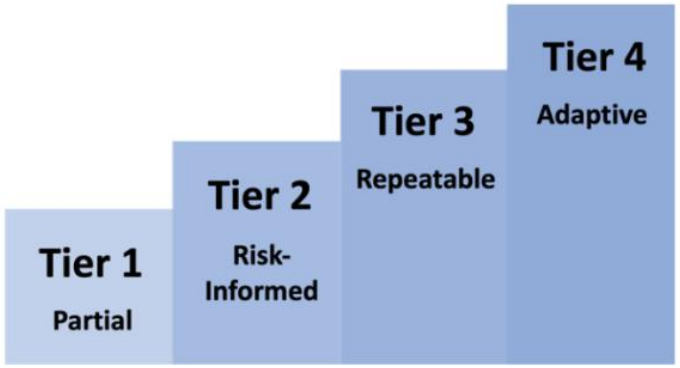
Proactive:

- **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