Modern Cyber and Technology Risk Measurement

Jack Jones
Chairman, The FAIR Institute

What we'll cover today…

- What's wrong and why it matters
- An introduction to FAIR
- Common concerns
- Measurement
- The hard part…
- Example analysis
- Practice analysis
- Wrapping it up

Organizations must prioritize their cyber risk problems and solutions.

Prioritization implies…

- Comparing their various concerns and solution options, which requires…
- Measurement

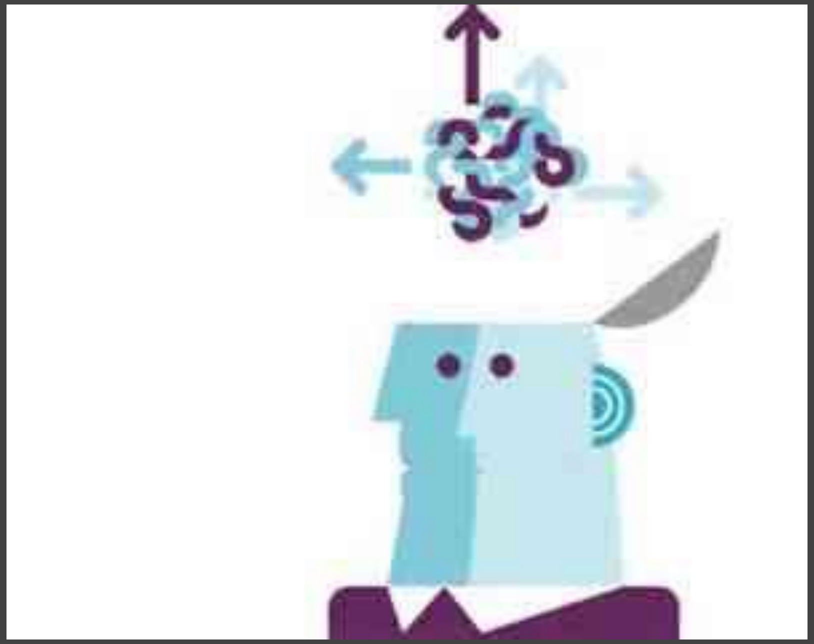
How is cyber risk being measured?

Just like any other complex measurement objective… by using a model and data.

An simple example is speed:

Speed = Distance/Time

What is the most commonly used cyber risk measurement model?



Mental models

A weak foundation

What are your organization’s top ten cyber risks?

What was #11, and how much less risk does it represent than #10?

Which of the following are risks?

- Disgruntled insiders
- Internet-facing web servers
- Untested recovery process
- Network shares containing sensitive consumer information
- Weak passwords
- Cyber criminals

Actually, none of them are risks

- Disgruntled insiders — Threat community
- Internet-facing web servers — Assets
- Untested recovery process — Deficient control
- Network shares containing sensitive consumer information — Assets
- Weak passwords — Deficient control
- Cyber criminals — Threat community

What is the classic formula for risk?

Risk = Likelihood x Impact

Likelihood and Impact of what?

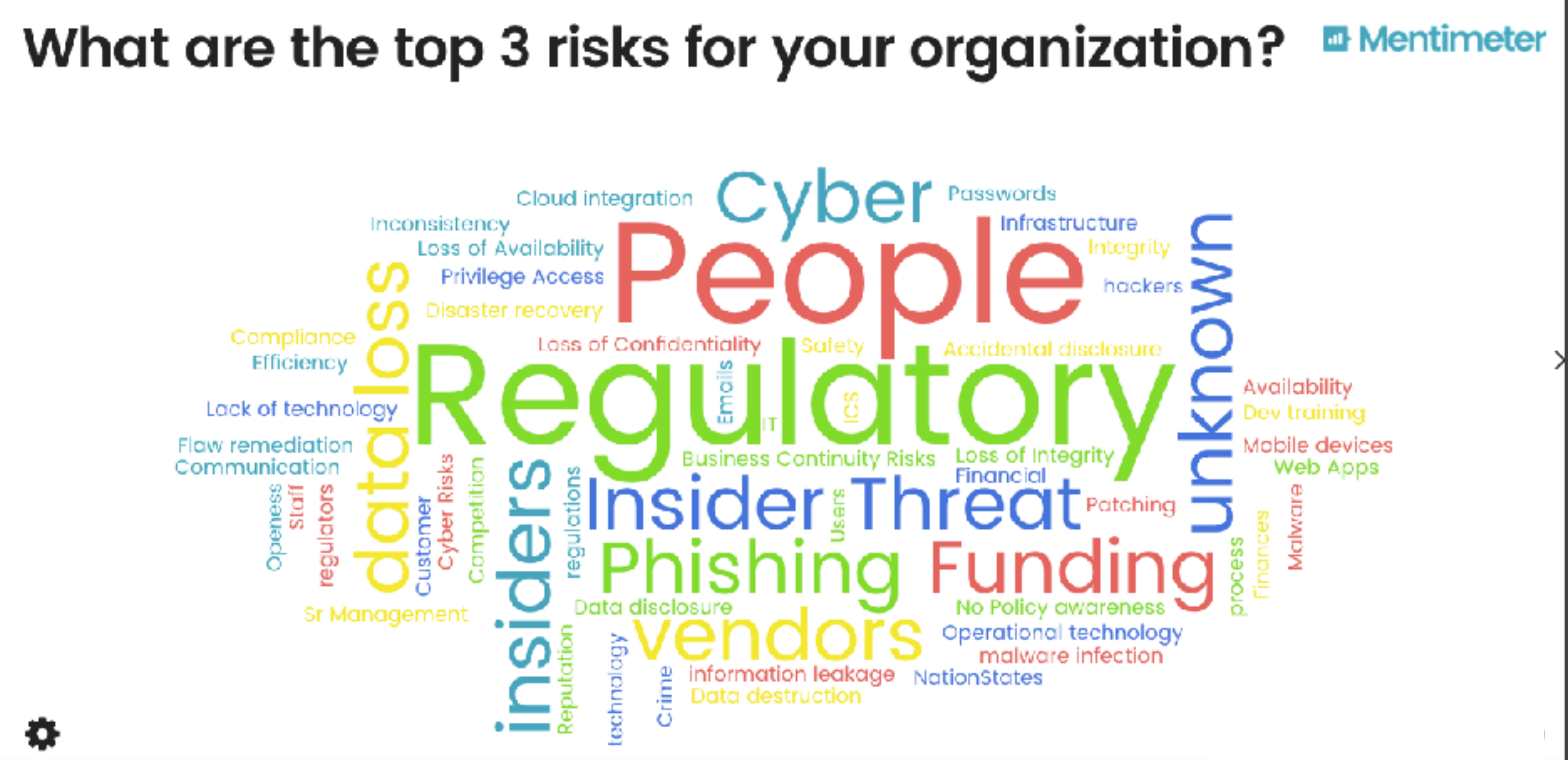
Loss Events

These aren't loss events

- Disgruntled insiders
- Internet-facing web servers
- Untested recovery process
- Network shares containing sensitive consumer information
- Weak passwords
- Cyber criminals

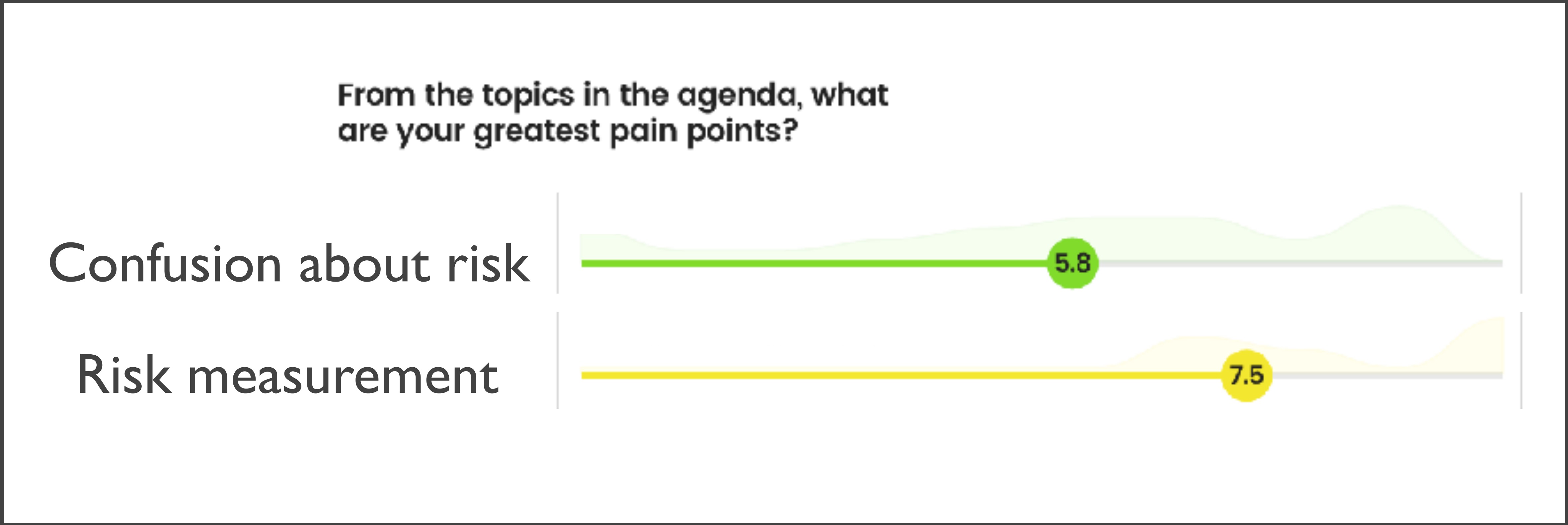
You can only assign likelihood and impact to loss events.

Infosec Risk Seminar Survey



What are the top 3 risks for your organization?

Infosec Risk Seminar Survey



From the topics in the agenda, what are your greatest pain points?

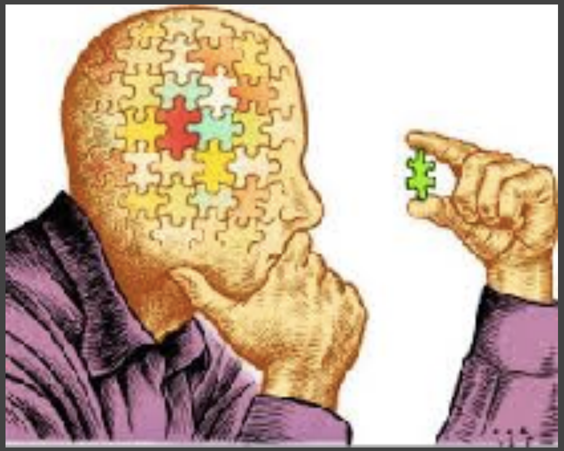
common

Other causes of inaccurate risk measurement

^

Absence of critical thinking

(Reliance on “best practices”)



Broken models

Focus on possibility vs. probability

common

Other causes of inaccurate risk measurement

^

Poorly defined measurement scales

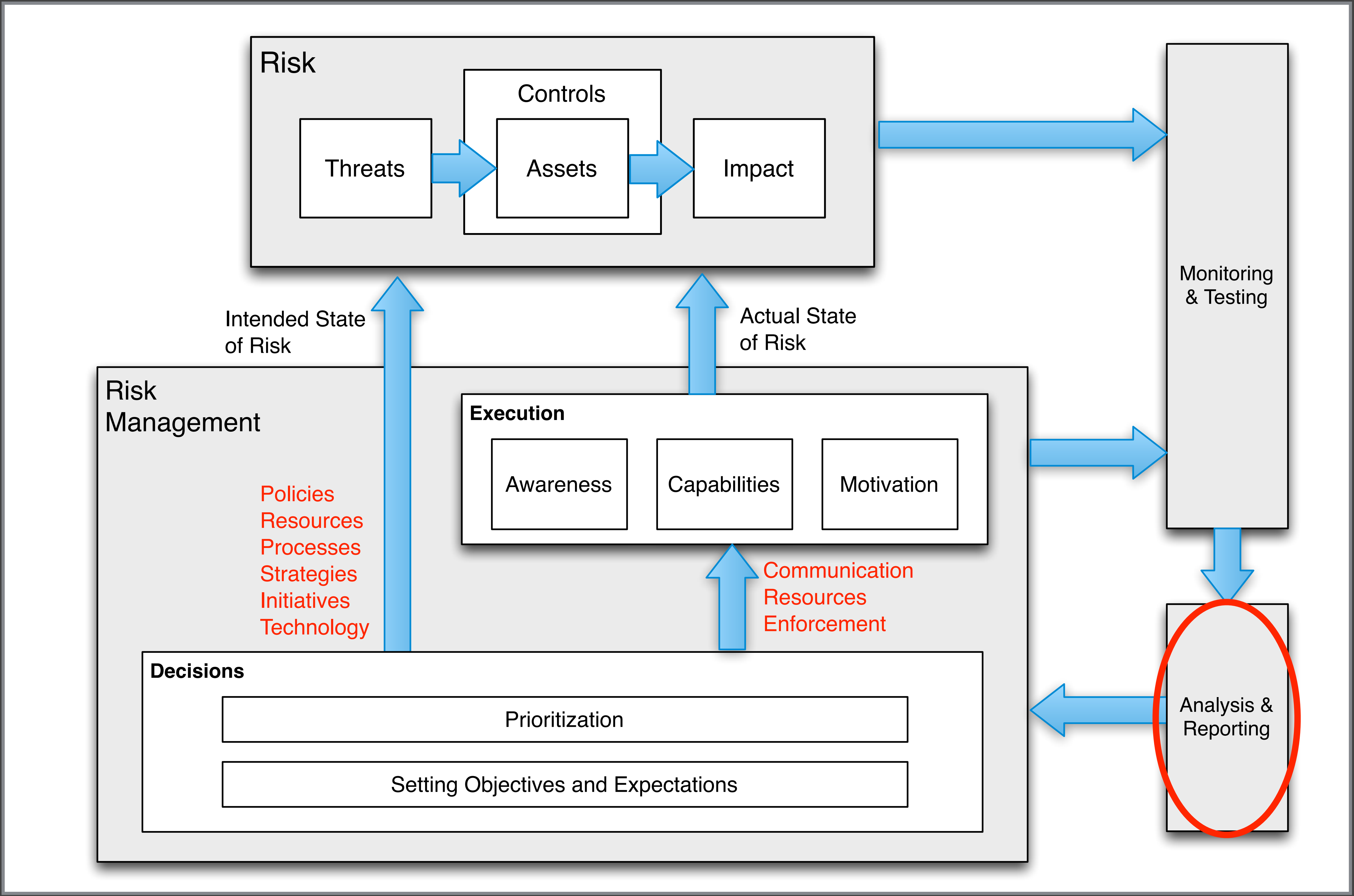
Bad estimates

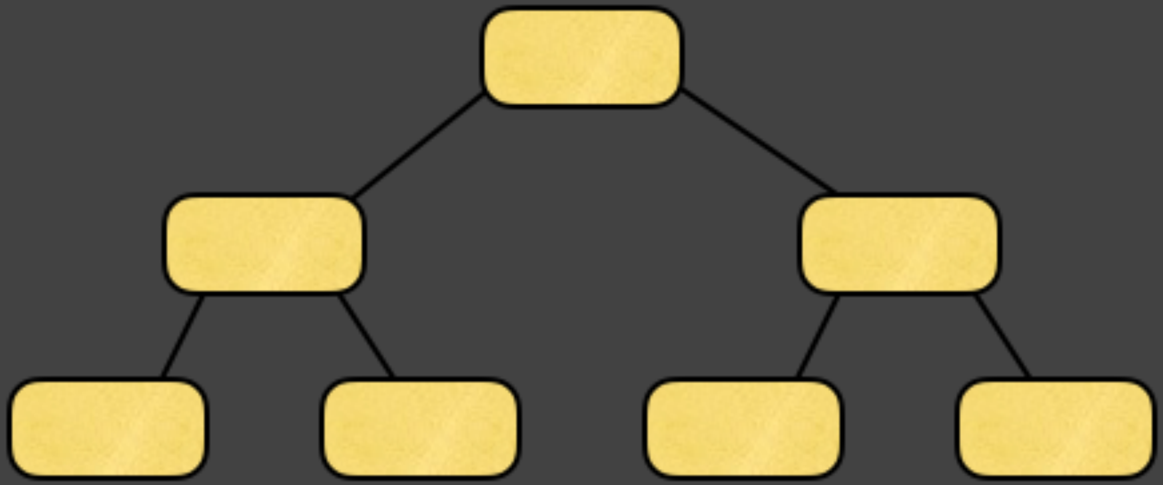
Math on
ordinal scales

(Red x Green) / Yellow = ?

70% to 90% of “high risk” issues, aren’t

Why it matters…





FAIR Ontology

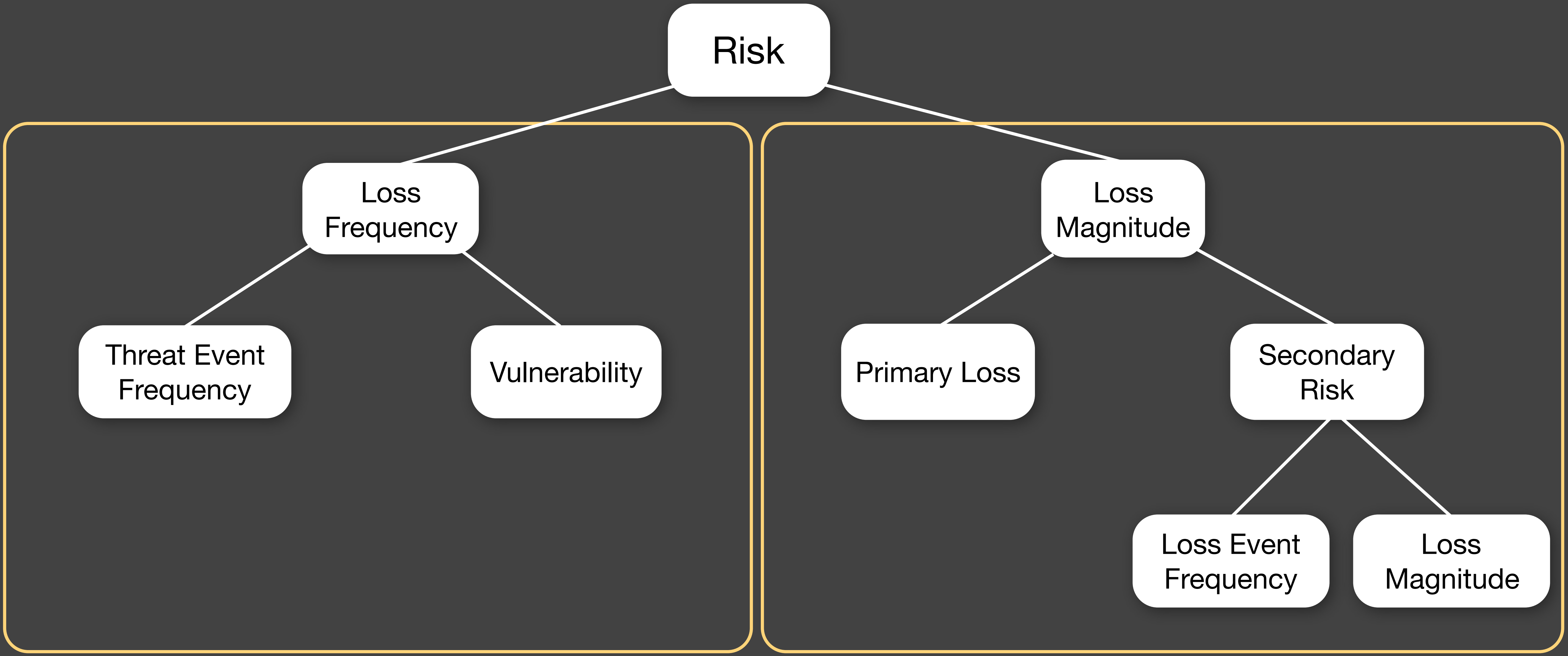
Risk...

The probable frequency and probable magnitude of future loss

In other words...

How often loss is likely to happen,
and how bad it's likely to be when it happens

FAIR Ontology



Risk

Loss Frequency

Threat Event Frequency

Vulnerability

Loss Magnitude

Primary Loss

Secondary Risk

Loss Event Frequency

Loss Magnitude

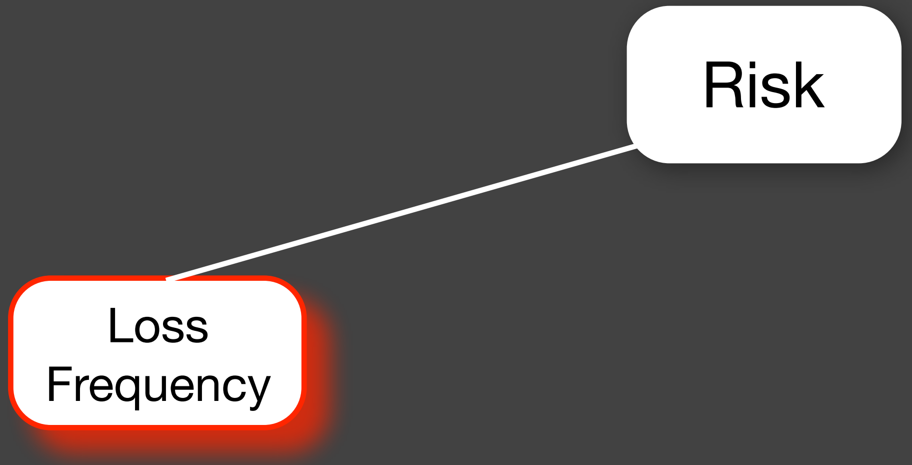
Probable
Loss Event Frequency

Probable
Loss Magnitude

Risk

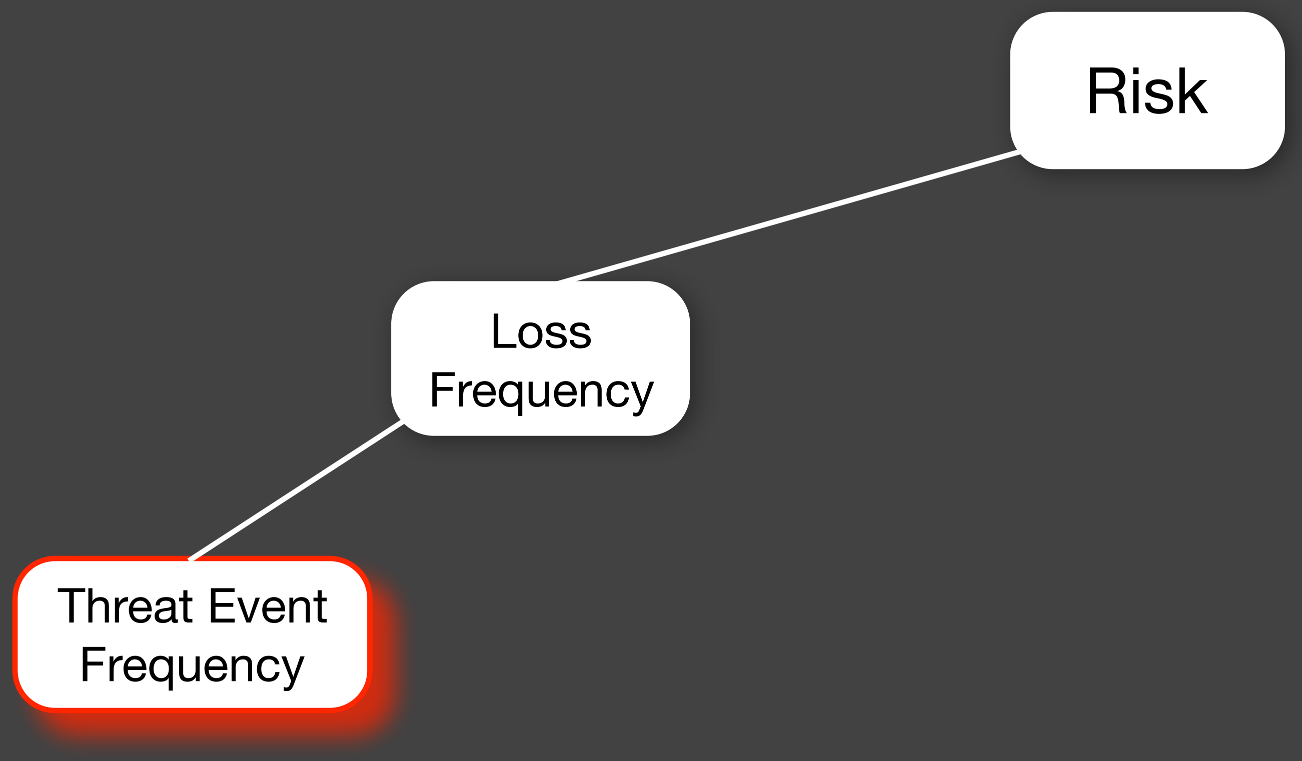
Risk

The probable frequency and probable magnitude of future loss



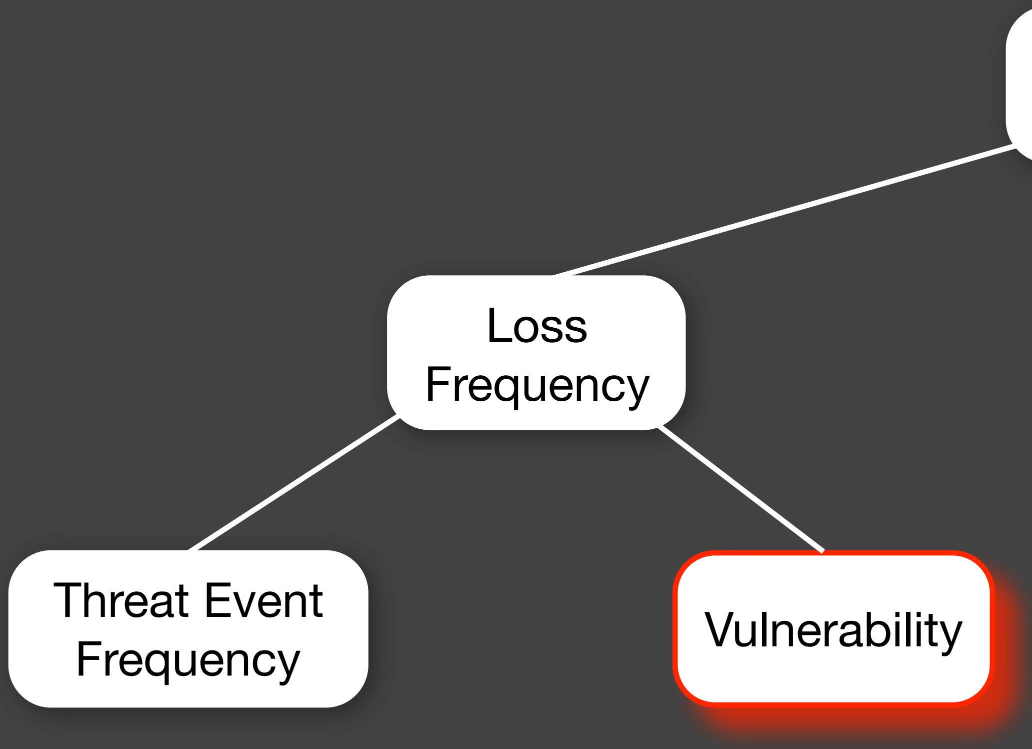
Loss Event Frequency

The probable frequency, within a given timeframe, that a threat action will result in loss



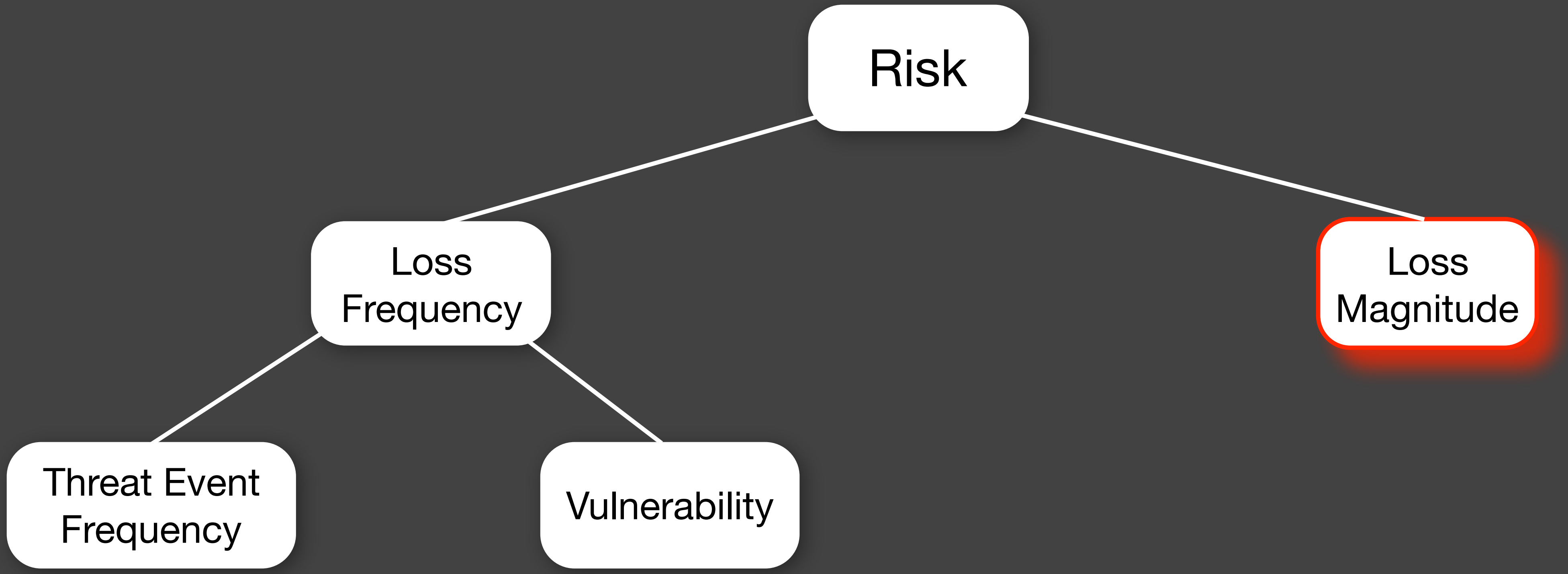
Threat Event Frequency

The probable frequency, within a given timeframe, that a threat will act in a manner that may result in loss



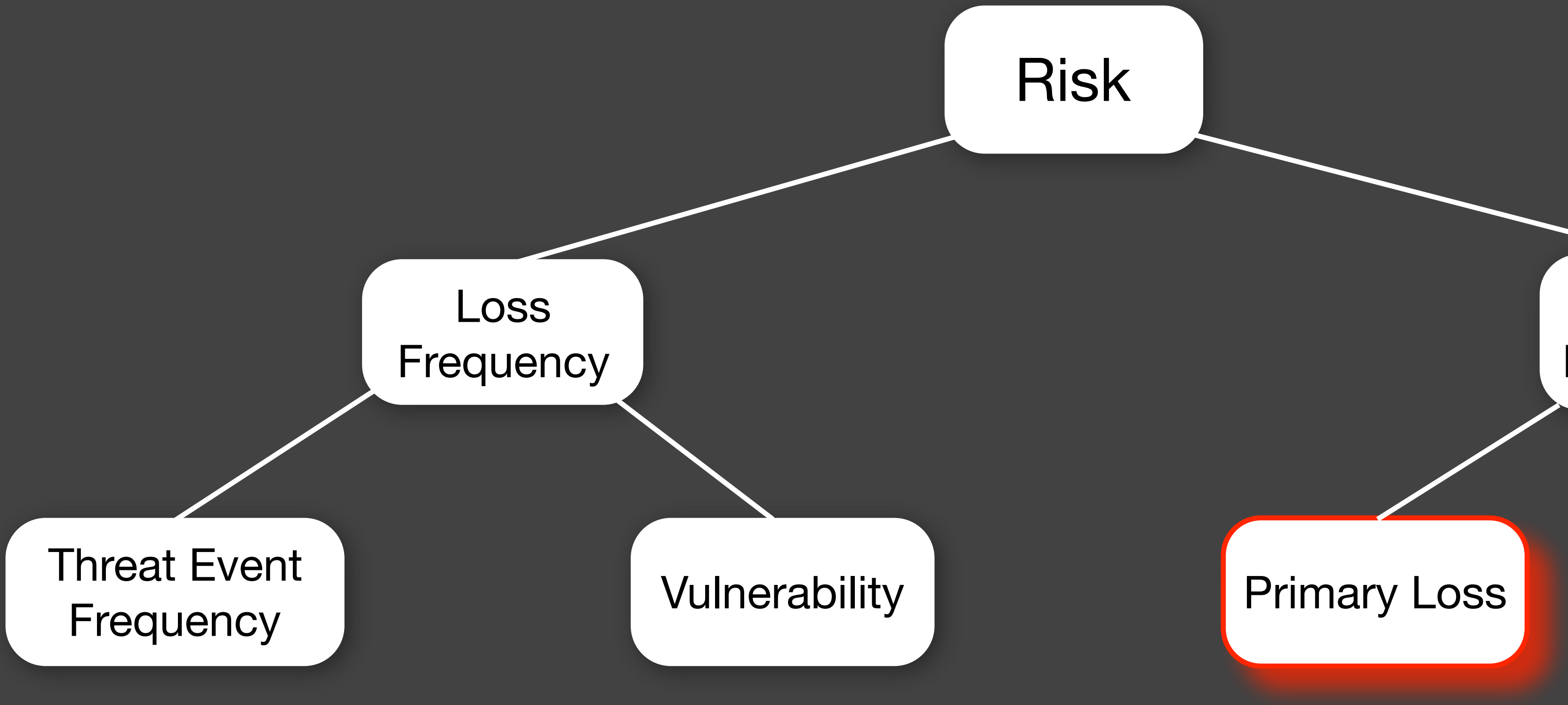
Vulnerability

The probability that a threat event will become a loss event



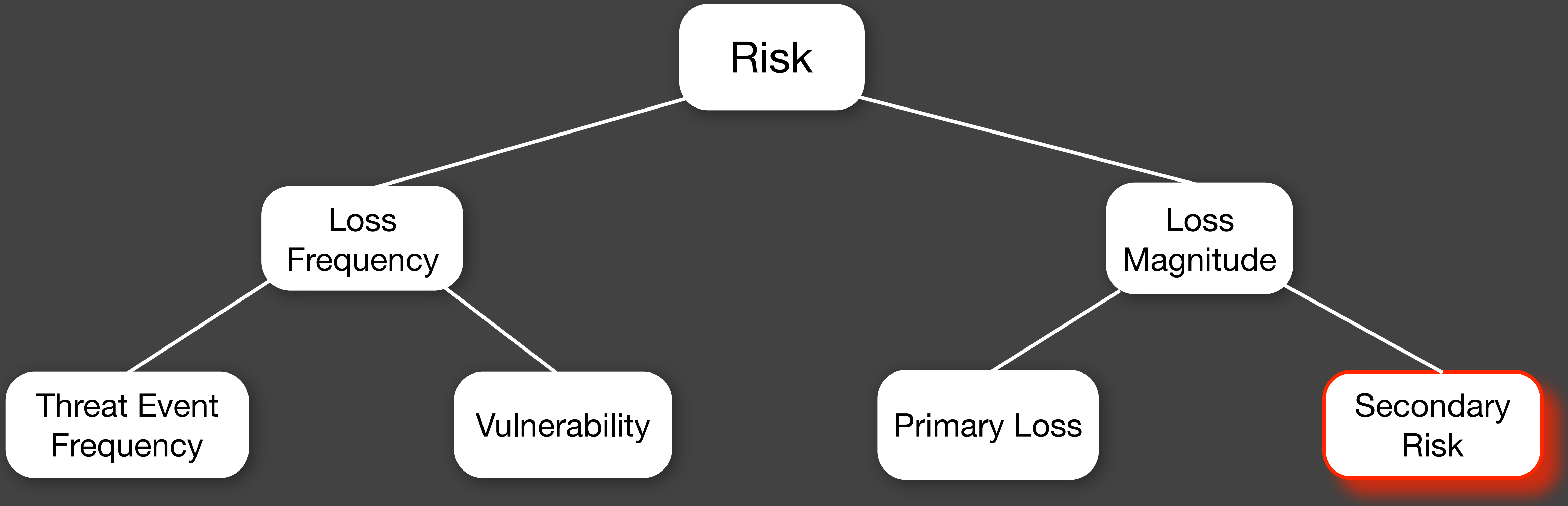
Probable loss magnitude

The probable magnitude of loss resulting from a threat action



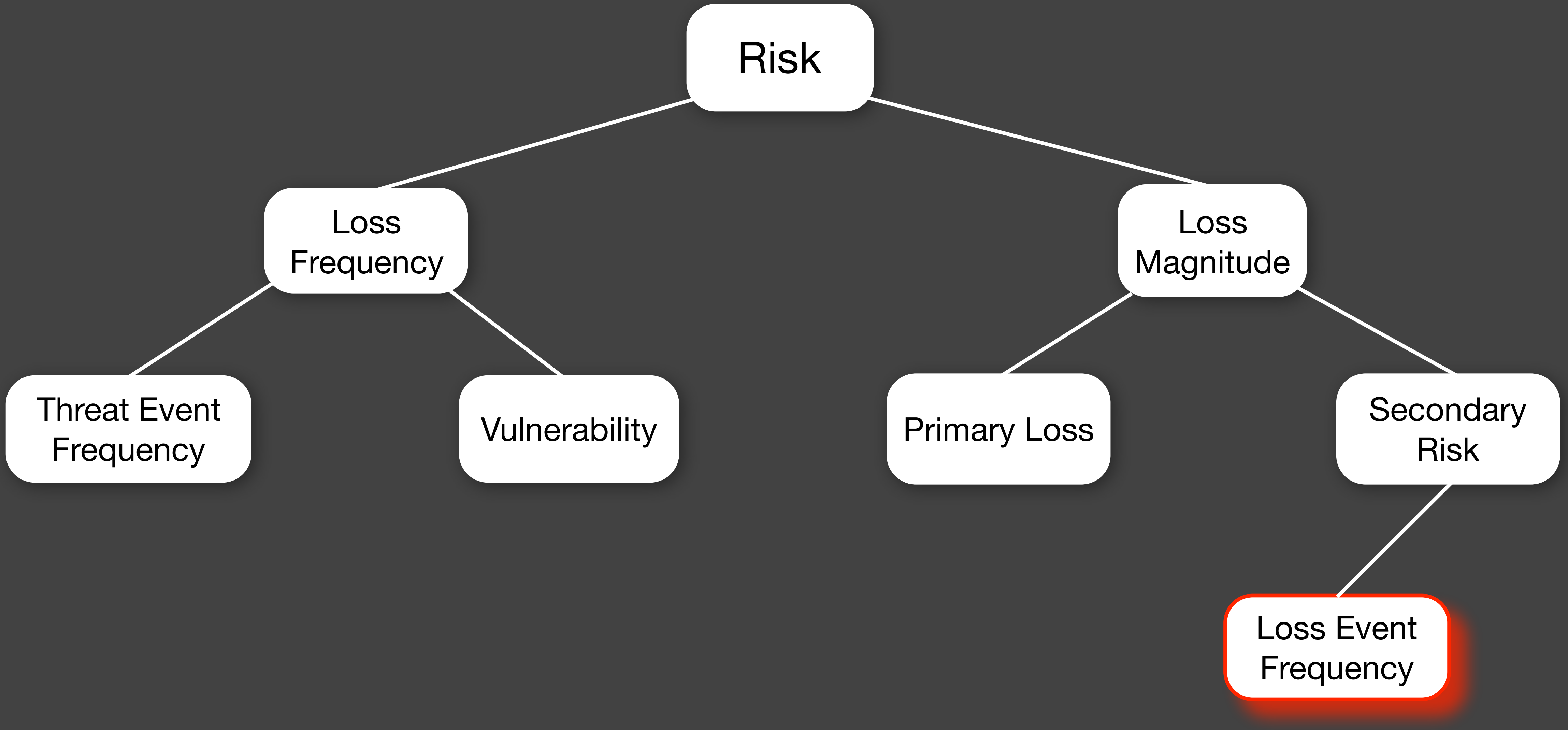
Primary loss

Loss that occurs directly as a result of the threat act against the asset.



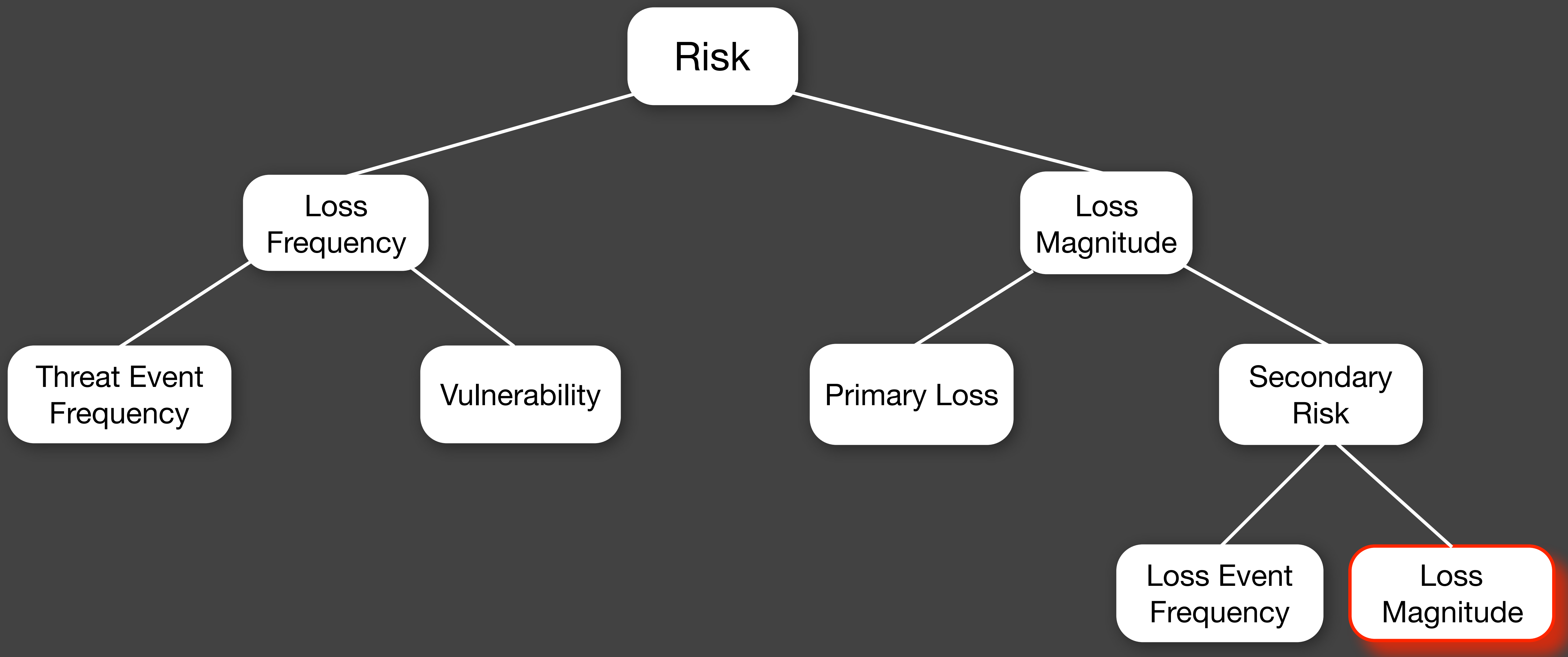
Secondary Risk

Loss that occurs as a result of secondary stakeholder reaction to the primary loss event.



Secondary LEF

The probable frequency of loss generated by secondary threats



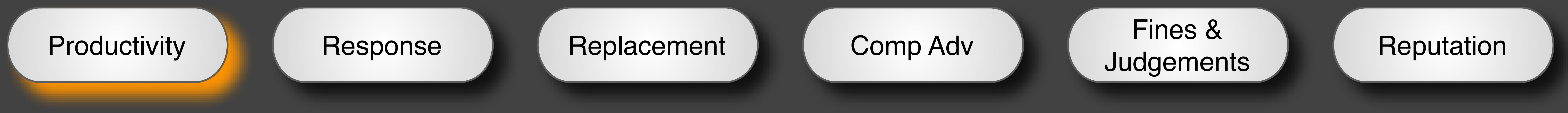
Secondary LM

The probable loss magnitude resulting from secondary threat actions

Forms of loss

- Productivity
- Response
- Replacement
- Comp Adv
- Fines & Judgements
- Reputation

Forms of loss



Productivity

Response

Replacement

Comp Adv

Fines & Judgements

Reputation

Productivity

Is the reduction in an organization’s ability to generate its primary value proposition (e.g., income, goods, services, etc.)

Forms of loss

Productivity | Response | Replacement | Comp Adv | Fines & Judgements | Reputation

Response

Expenses associated with managing a loss event (e.g., internal or external person-hours, logistical expenses, etc.)

Forms of loss

Productivity

Response

Replacement

Comp Adv

Fines & Judgements

Reputation

Replacement

The intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost or damaged assets (e.g., rebuilding a facility, purchasing a replacement laptop, etc.)

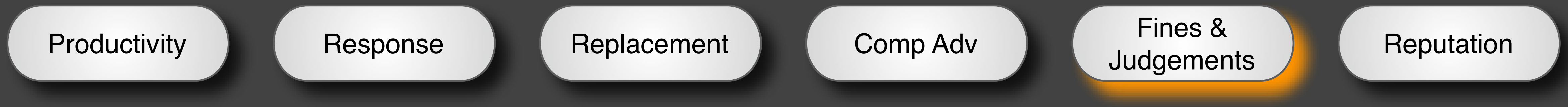
Forms of loss

Productivity | Response | Replacement | Comp Adv | Fines & Judgements | Reputation

Competitive Advantage

Losses associated with diminished competitive advantage. CA loss is specifically associated with assets that provide competitive differentiation between the organization and its competition. Examples would include trade secrets, merger and acquisition plans, etc.

Forms of loss



Productivity

Response

Replacement

Comp Adv

Fines & Judgements

Reputation

Fines & Judgments

Legal or regulatory actions levied against an organization. Note that this includes bail for any organization members who are arrested.

Forms of loss

Productivity | Response | Replacement | Comp Adv | Fines & Judgements | **Reputation**

Reputation

Losses associated with an external perception that an organization’s value proposition is reduced or leadership is incompetent, criminal, or unethical.

But…

Common concerns

Isn’t quantifying cyber risk different and harder (or even impossible)?

What are some of the reasons for this concern?

How does qualitative measurement solve/avoid those concerns?

A simple estimation problem

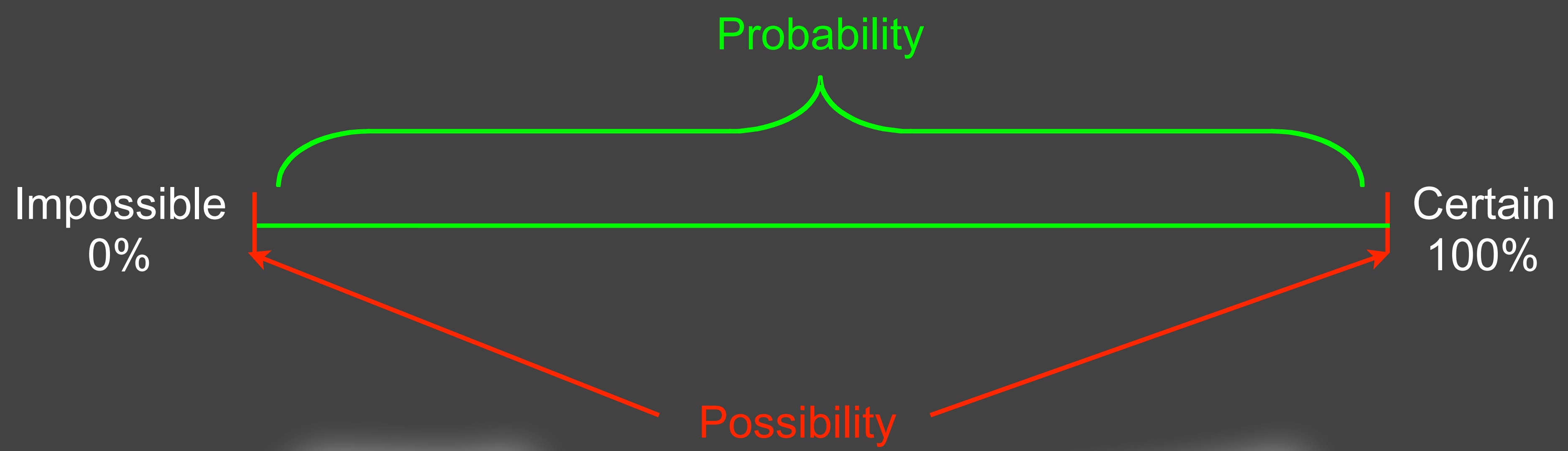
- How fast is the car going?
  - Qualitatively
  - Quantitatively

Oh look! It fits!

Qualitative and ordinal risk measurements are subject to the same challenges as quantitative measurements, they just sweep the problems under the rug rather than force us to deal with them.

Probability vs. Prediction

Probability vs. Possibility



Probability

Impossible
0%

Certain
100%

Possibility

~17%

~100%

The dirty word of measurement: **SUBJECTIVITY**

Objective

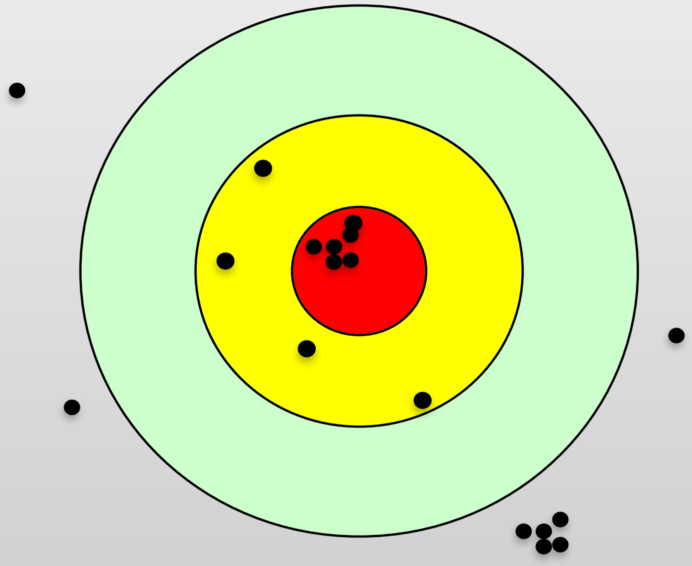
Subjective

Reality

Precision vs. Accuracy

What we aim for…

What we typically see…



Inaccurate & Imprecise
Inaccurate & Precise
Accurate & Precise
Accurate & Imprecise

Measurement

Estimating

- How tall am I?
  - 5’5”
  - 5’6”
  - 5’7”
  - 5’8”
  - 5’9”
  - 5’10”
  - 5’11”
  - 6’0”
  - 6’1”
  - 6’2”

Would you bet $1,000 on your estimate?

Was that estimate subjective or objective?

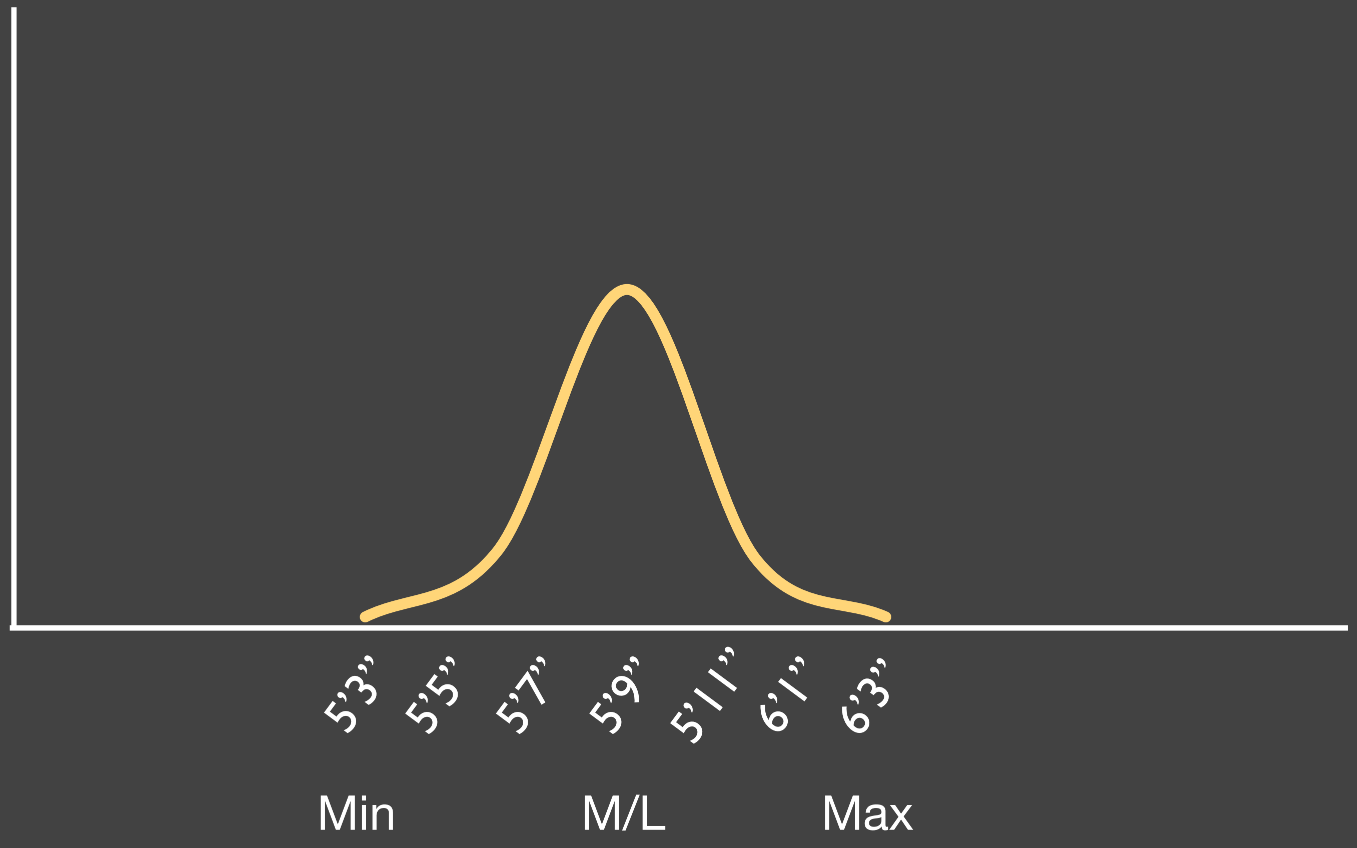
Estimating using ranges

- How tall am I?
  - < 5’5”
  - 5’5” - 5’11”
  - 6’0” - 6’6”
  - < 6’6”

We achieve accuracy with an acceptable level of precision.

Estimating using distributions

- How tall am I?



What is calibration?

A method for measuring and improving an individual’s ability to make good estimates

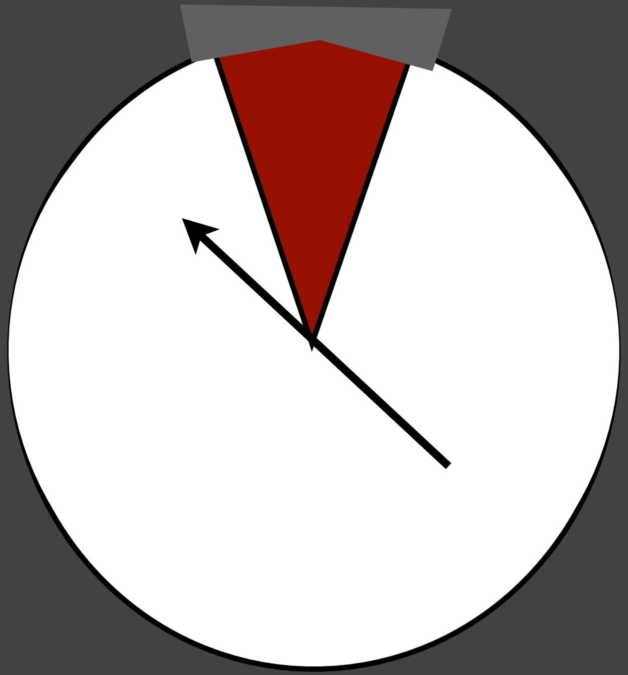
Why calibration?

- Garbage in, garbage out...
- The ability to estimate effectively varies from person to person
- People can be trained to estimate more effectively

Example

What is the wingspan of a Boeing 747?

- 1 to 1000 feet?
- 50 to 500 feet?
- 100 to 300 feet?
- 125 to 250 feet?



Practice

Question	Min	Max
How many gallons are in a bushel?	8	
How many sovereign rulers has England had in the past thousand years?	47	
How many meters tall is the Sears Tower?	443	
What is the average daily calorie intake (per person) in developed countries?	3300	

Benefits of calibration

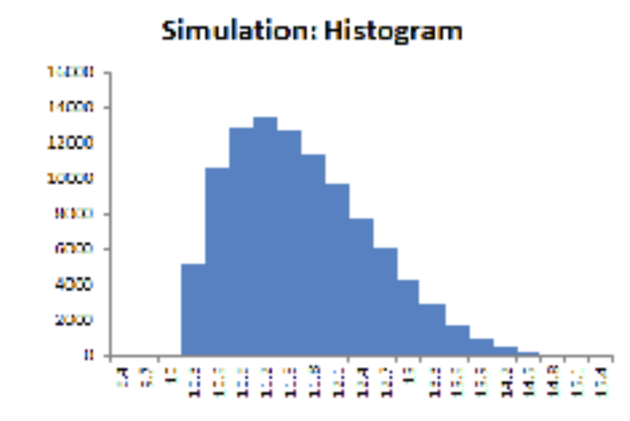
- Reduces the probability of gross error
- Surfaces assumptions
- Establishes the basis/rationale for estimates
- Provides values that can be plugged into Monte Carlo or other analytic functions

Monte Carlo Simulations

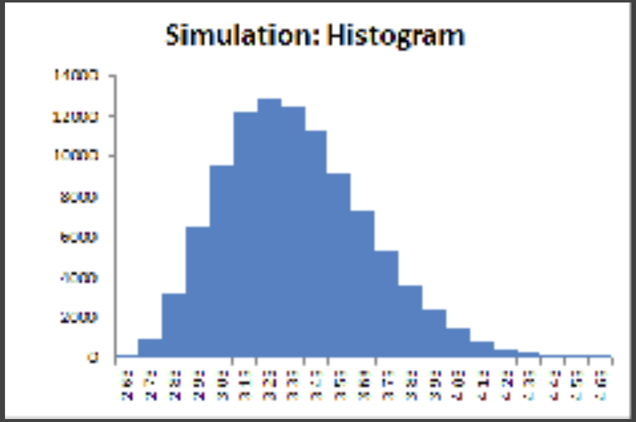
Combining uncertain values

- Speed = Distance / Time
- How to derive speed when distance and/or time measurements have some amount of uncertainty or variability?

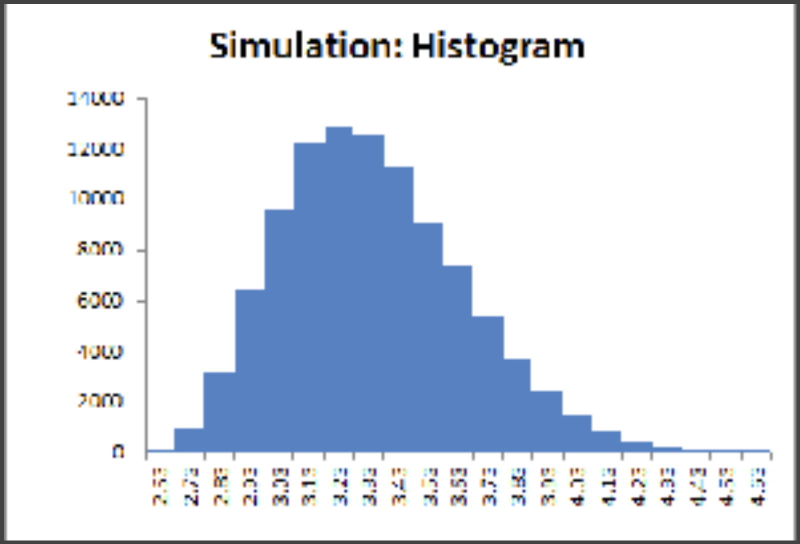
- Distance:
  - Min: 10 mile
  - Max: 15 miles
  - ML: 11 miles



- Time:
  - Min: 3 hours
  - Max: 4 hours
  - ML: 3.5 hours

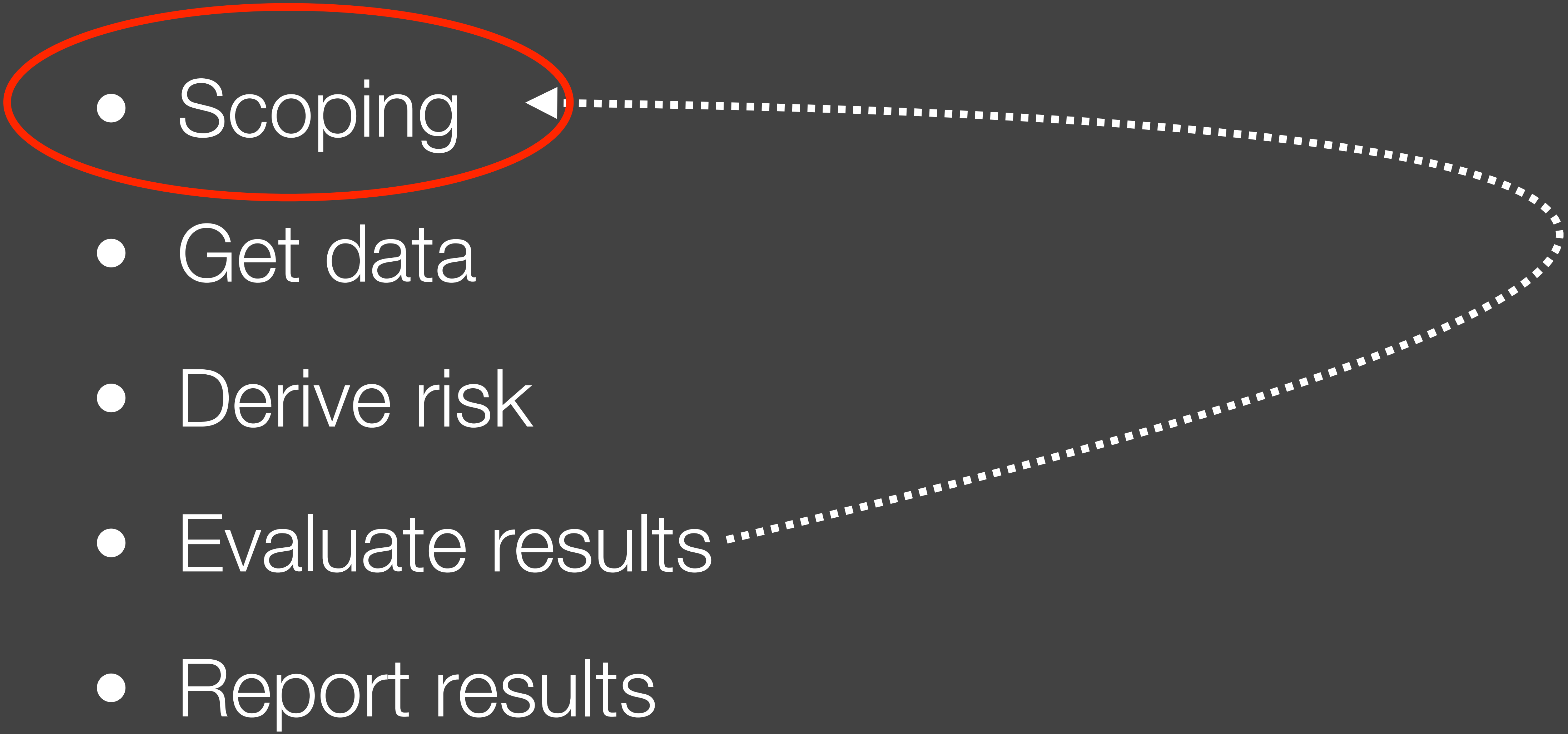


Speed



The Hard Part…

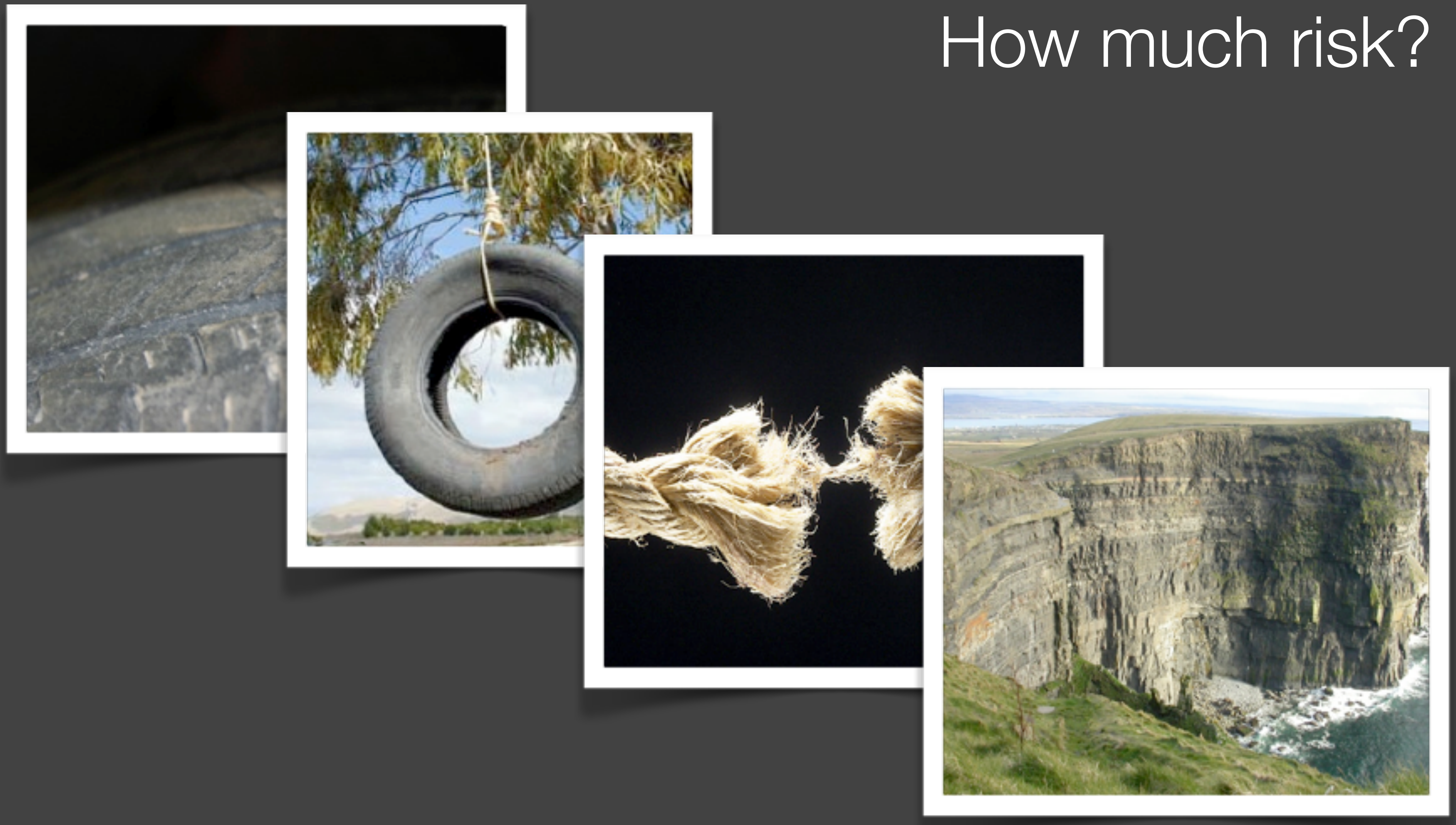
The analysis process



- Scoping
- Get data
- Derive risk
- Evaluate results
- Report results

Bald Tire

How much risk?



There will always be assumptions in any analysis.

The key is to surface them.

Scoping - step 1

- What is the loss event (risk) we're trying to understand/measure?
  - Compromise of sensitive information?
  - Loss of availability?
  - Project cost-overrun?

Scoping - step 2

- What is/are the relevant asset(s)? Where does the loss event occur?
  - Laptop?
  - Server?
  - Web application?
  - Network transmission?

Scoping - step 3

- Who/what is the relevant threat?
  - Cyber criminals?
  - Privileged insiders?
  - Mother nature?
  - Customers?
  - Technology?

Scoping - step 4

- What type of threat event is it?
  - Accidental?
  - Intentional but not malicious?
  - Intentional and malicious?
  - Other?

Scoping - step 5

- In what manner does the threat event occur (vector)?
  - Over the network?
  - Locally to the system?
  - Direct physical contact?
  - Through an unwitting accomplice?

Without this kind of scoping rigor, the odds of measuring risk accurately are much lower, regardless of whether you’re doing qualitative or quantitative measurement

Example Analysis

An audit discovered that privileges for accounts in the customer support application aren’t consistently being updated when personnel change roles.

Gut check

- Is this a risk?
- Why or why not?
- How much risk does this represent?

Scoping this analysis…

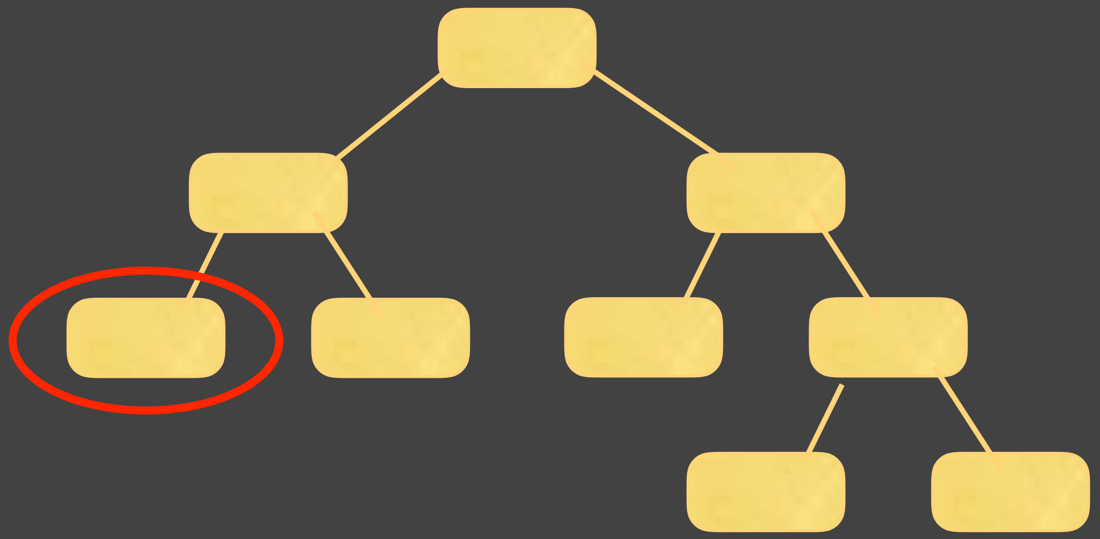
- What is the asset at risk? Customer information
- Who/what is the threat actor(s)? Personnel with inappropriate access
- What type of action Malicious
- What type of event is it (C, I, or A)? Confidentiality
- What is the loss event? The confidentiality of customer data is maliciously compromised by an employee with inappropriate access

This is the risk

Threat Event Frequency

- Definition

  The probable frequency, within a given timeframe, that a threat will act in a manner that may result in loss



Who is the threat agent?

- Estimates

  Qualitative?

  Min: .05 yr (1 in 20 yr)

  ML: .1 yr (1 in 10 yr)

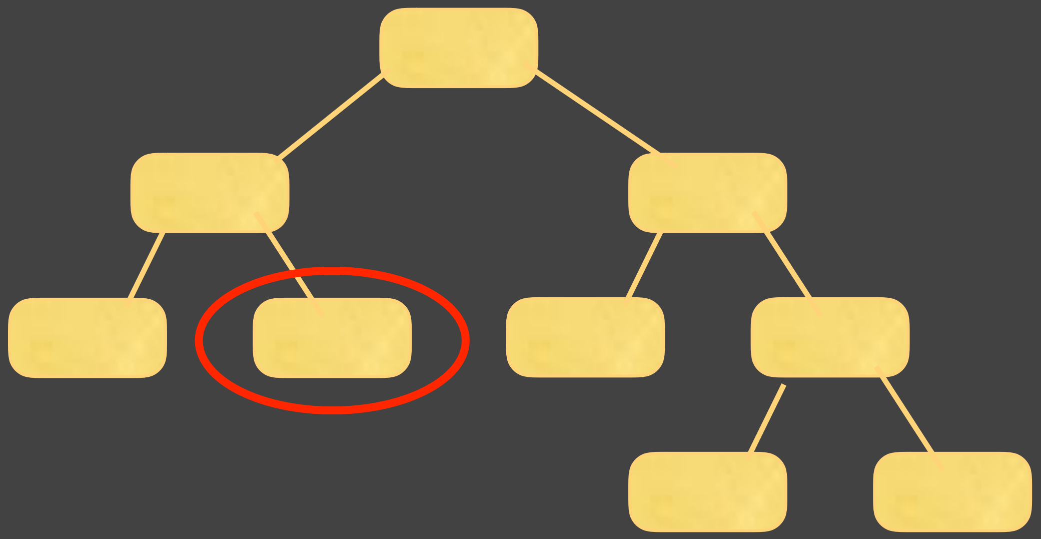
  Max: 5 yr

- Data/Rationale
  - 30 user accounts (out of 200) with inappropriate access levels (15%)
  - HR records show 2 events of misuse in the past 3 yrs ("snooping")
  - Snooping was performed by personnel with appropriate access
  - No history of malicious misuse

Vulnerability

- Definition

The probability that a threat event will become a loss event



- Estimates

Qualitative?

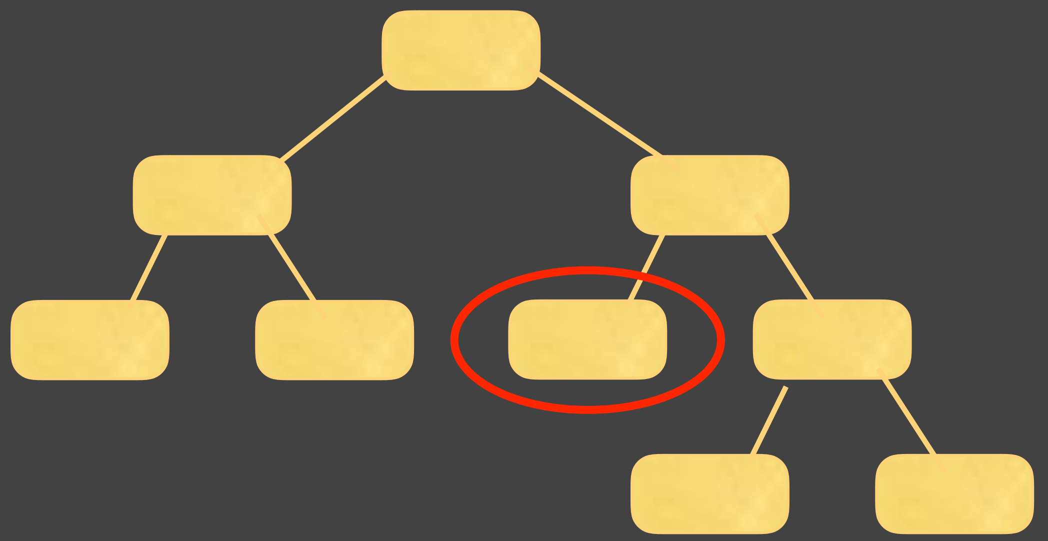
100%

- Data/Rationale
  - These are privileged insiders who don’t have to overcome controls in order to execute the illicit action

Primary Loss Magnitude

- Definition

Loss that occurs directly as a result of the threat act against the asset.



- Estimates

Qualitative?

Min: $ 25k

ML: $ 40k

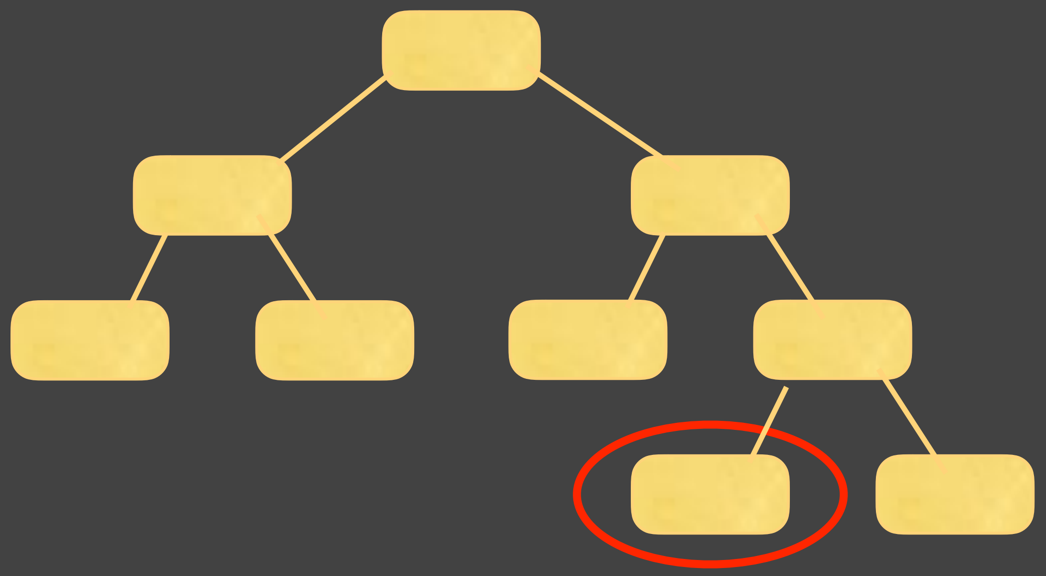
Max: $ 150k

- Data/Rationale
  - Combination of forensic/investigative costs and costs associated with replacing the malicious employee

Secondary Loss Event Frequency

- Definition

The probable frequency of loss generated by secondary threats



- Estimates

Qualitative?

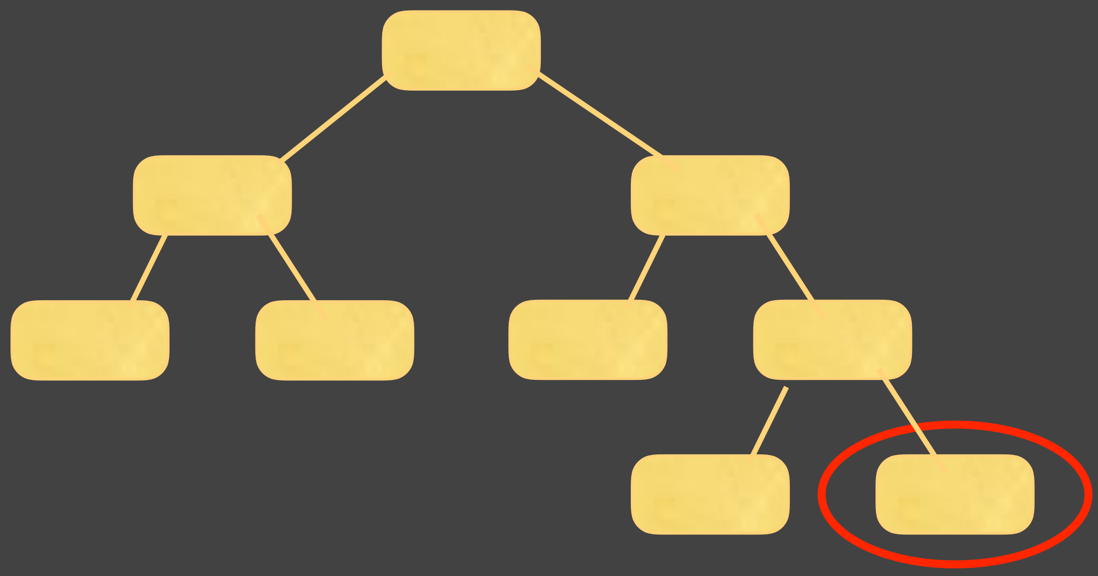
100%

- Data/Rationale
  - Assumes that any compromise of customer information would require notification and other secondary costs

Secondary Loss Magnitude

- Definition

The probable loss magnitude resulting from secondary threat actions



- Estimates

Qualitative?

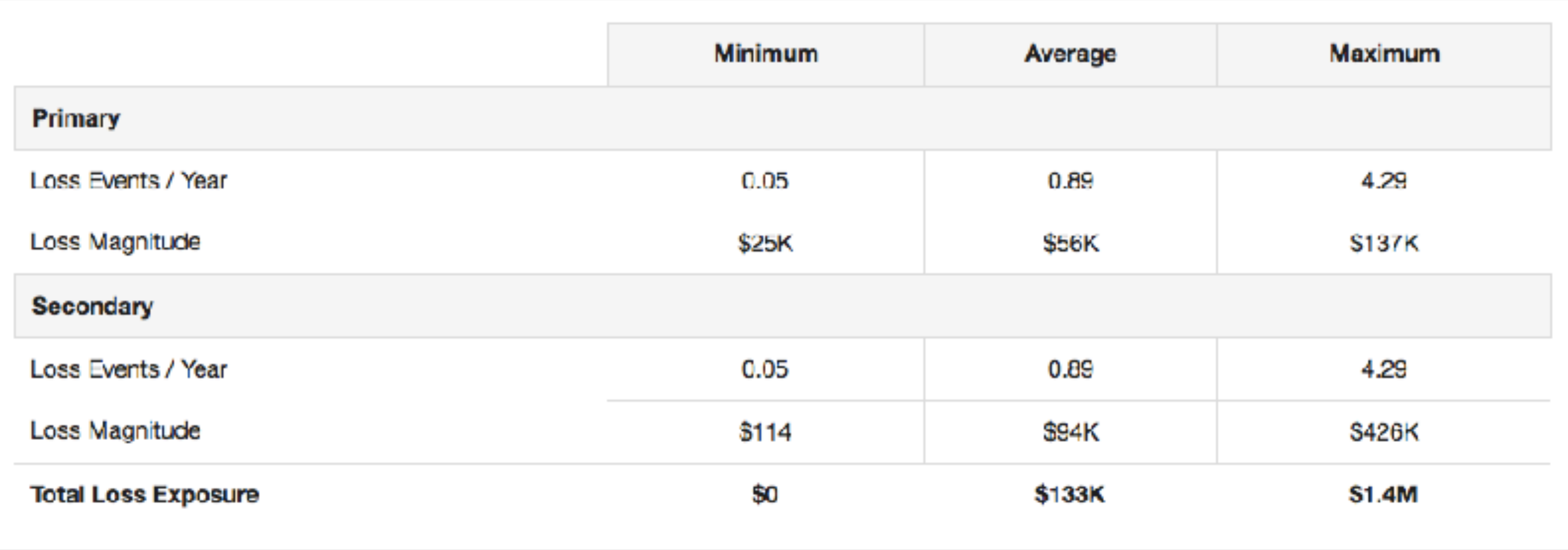
Min:	$ 100
ML:	$ 17k
Max:	$ 500k

- Data/Rationale
  - Minimum of 1 customer record
  - Most Likely 20 customer records
  - Maximum 100 customer records due to user account access limitations
  - Includes notification costs, credit monitoring, legal defense, and customer churn

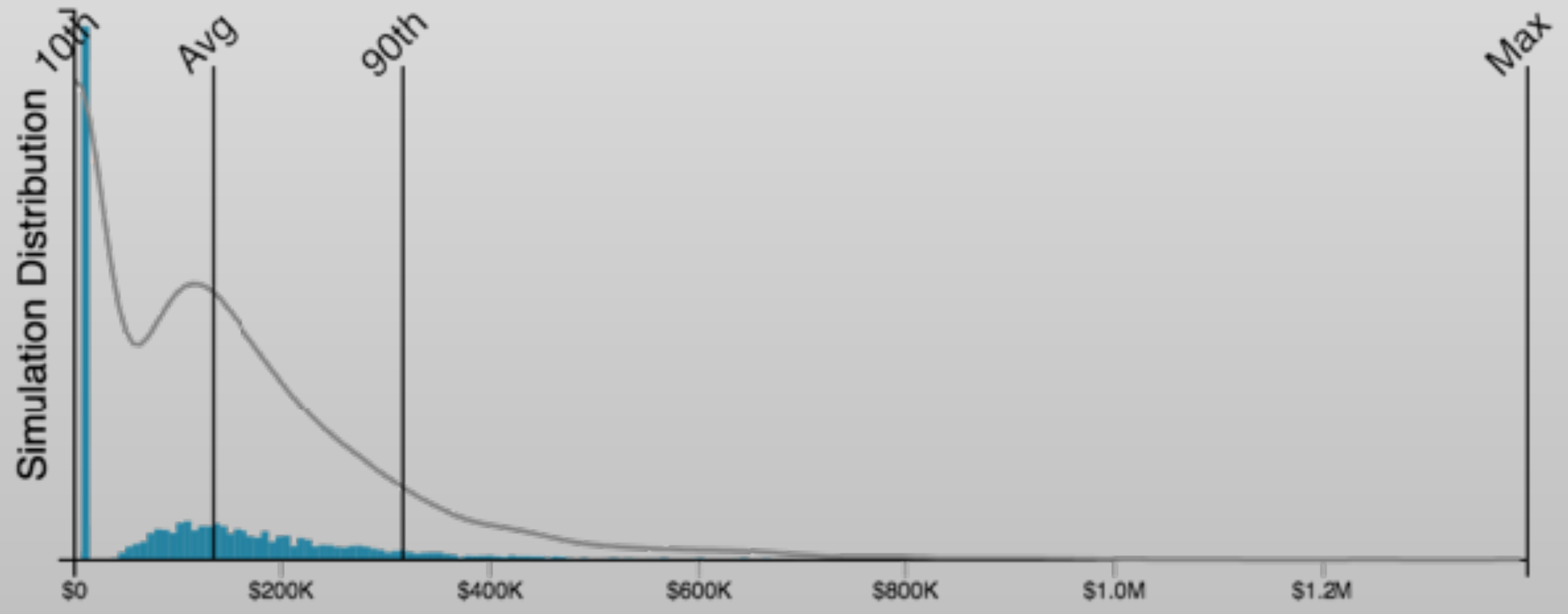
Qualitative results…

- High?
- Medium?
- Low?

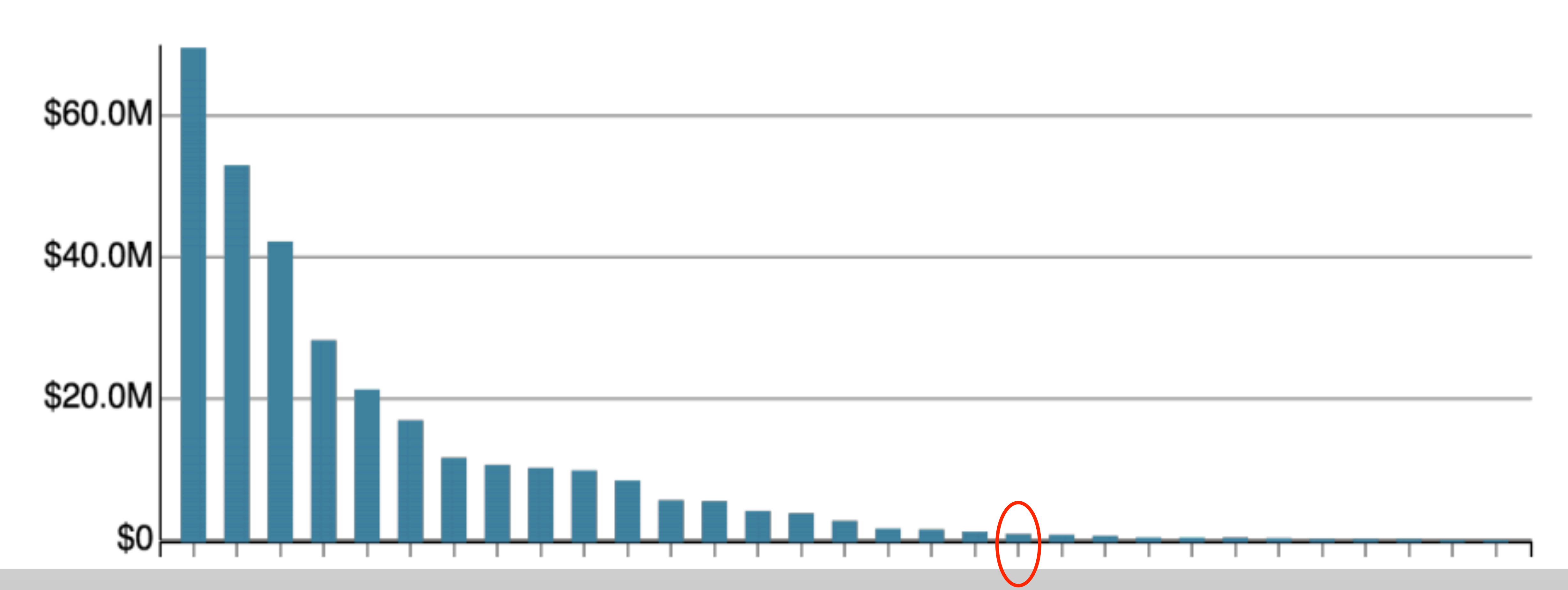
Analysis results



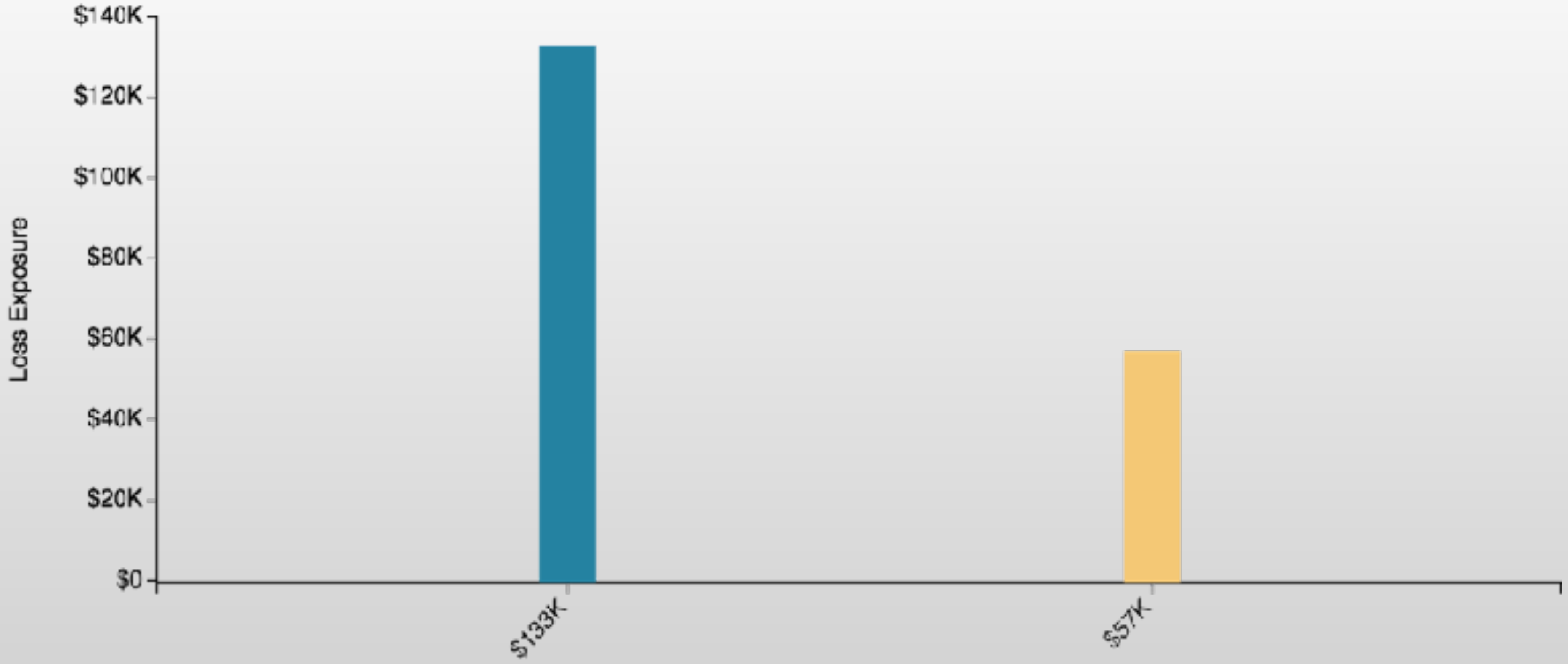
	Minimum	Average	Maximum
Primary			
Loss Events / Year	0.05	0.89	4.29
Loss Magnitude	$25K	$56K	$137K
Secondary			
Loss Events / Year	0.05	0.89	4.29
Loss Magnitude	$114	$94K	$426K
Total Loss Exposure	**$0**	**$133K**	**$1.4M**

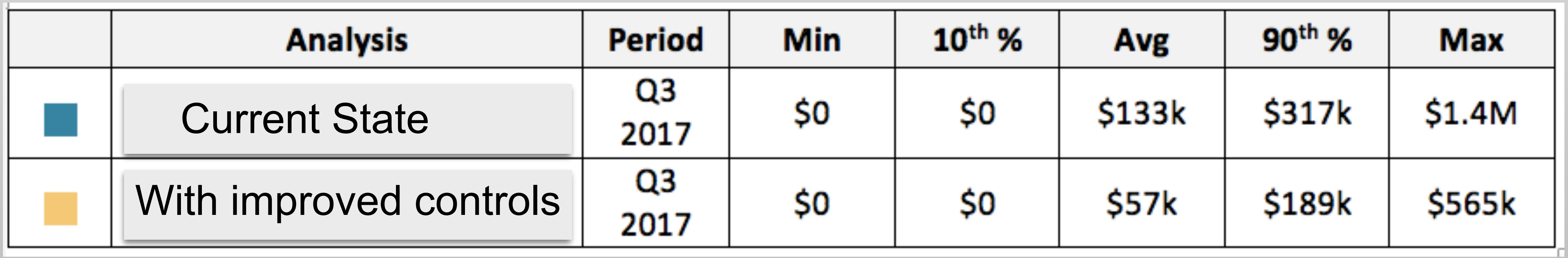


Prioritization



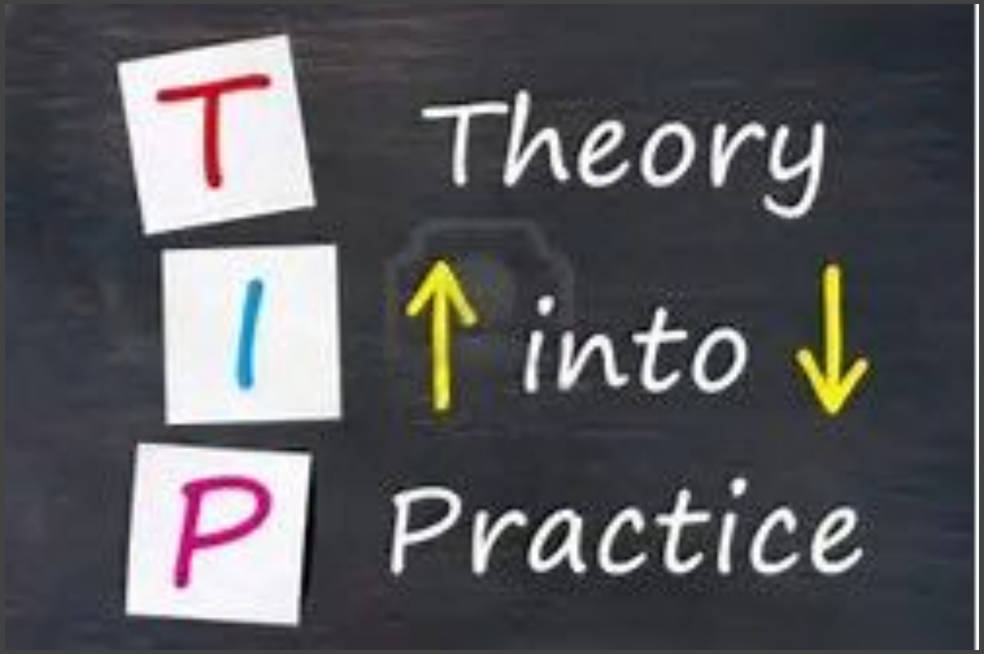
Mitigation benefit analysis



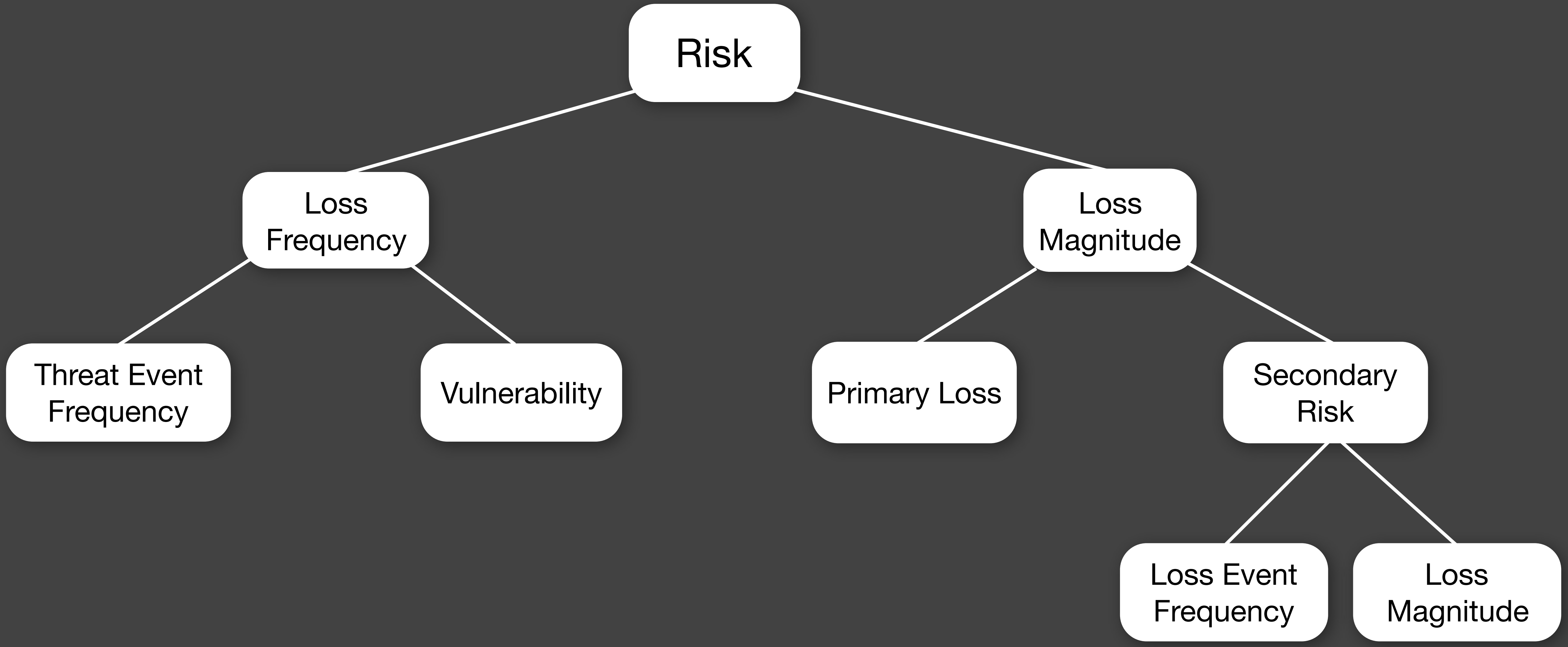


	Analysis	Period	Min	10th %	Avg	90th %	Max
🟦	Current State	Q3 2017	$0	$0	$133k	$317k	$1.4M
🟨	With improved controls	Q3 2017	$0	$0	$57k	$189k	$565k

Let’s do an analysis…



FAIR Ontology



Controls?

What risk do we want to measure?

Spreadsheet tool

- http://bit.ly/2y1eqGn
- Will take you to an Excel spreadsheet on box.com

Wrapping it up

FAIR Advantages

- Improves risk measurement and prioritization/focus (whether qualitative or quantitative)
  - Provides a framework for critical thinking
  - Normalizes terminology and mental models
- Improves the ability to speak in business-risk terms and establish useful risk appetite thresholds
- Complements common “good practice” frameworks
- Can be used to analyze any form of risk
- Reduces religious arguments
- Is an open international standard (The Open Group)

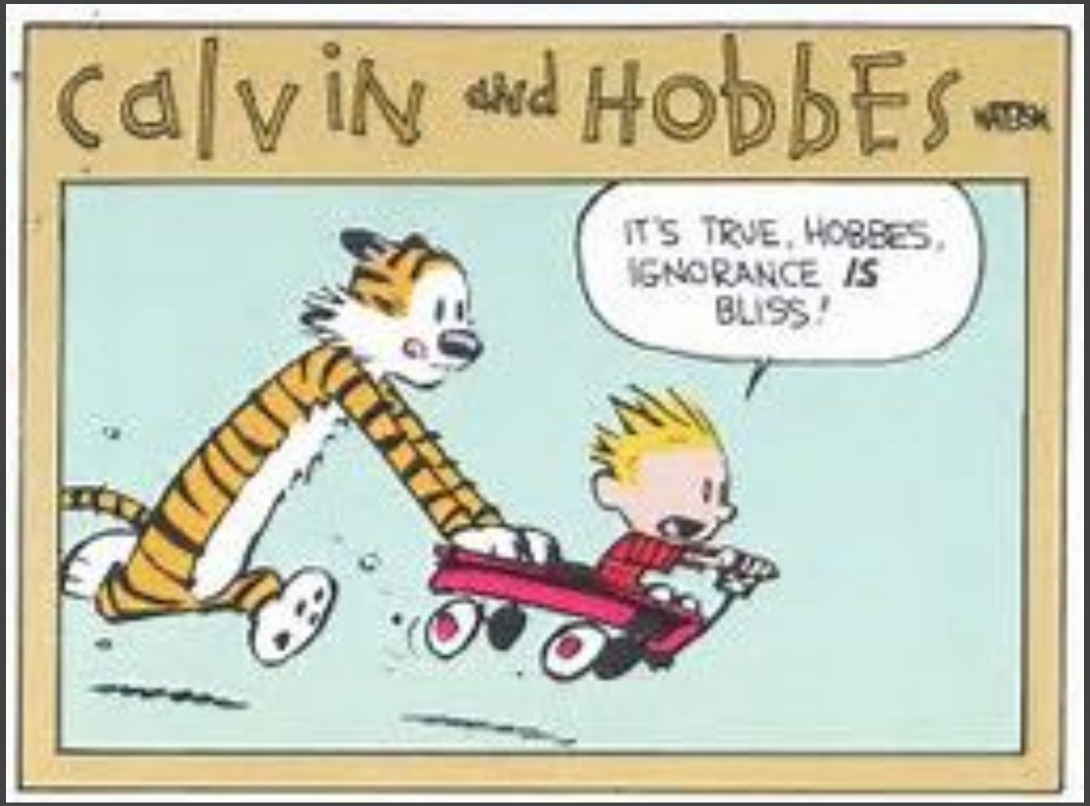
Maturity concerns

- “We’re not mature enough to do quantitative risk analysis”
- “We don’t have enough data”

Minimal adoption approach

- Adopt the ontology as a standard risk model for your organization
    - Normalizes terminology
    - Normalizes mental models
- Adopt the scoping principles
- Assign specific responsibilities
    - Not everyone is cut out to do risk analysis
    - Requires
        - Critical thinking skills
        - Being comfortable with uncertainty
        - Awareness of basic probability principles

Remember the red pill/blue pill thing?

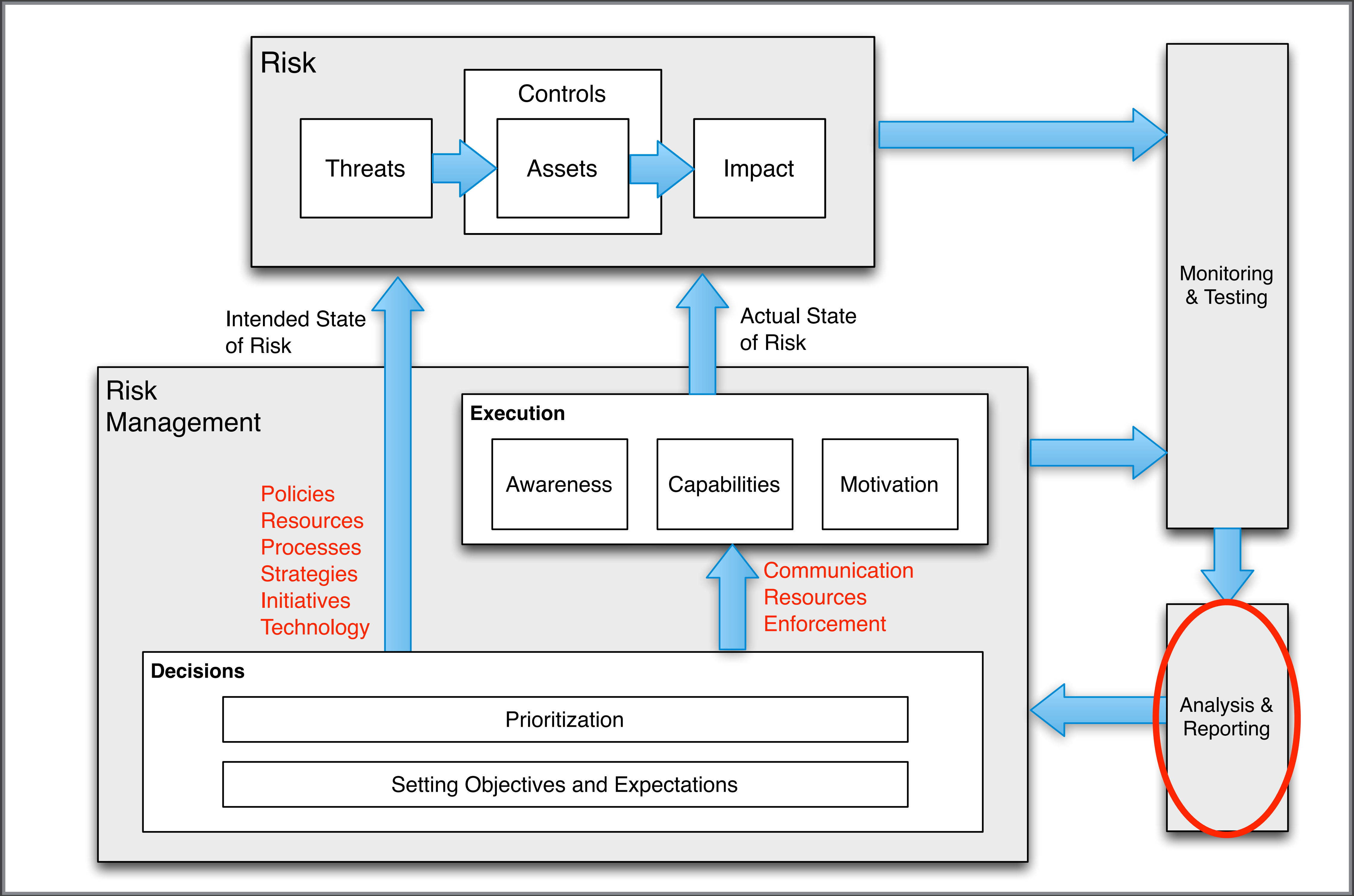


Ignorance is bliss…

…but you're no longer ignorant

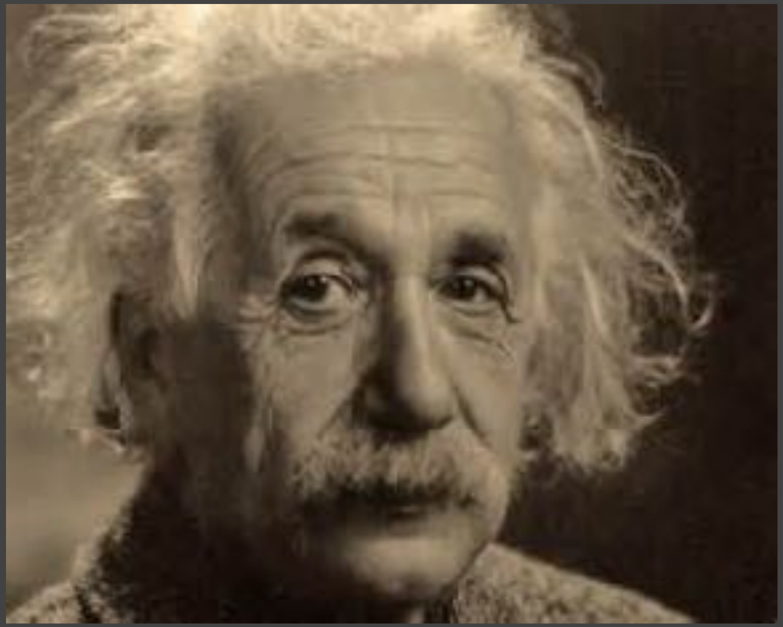
- From this point forward, you can choose to ignore what I’ve shared, but you’re no longer ignorant of the issues.
- Or, you can become a change agent by:
  - Seeking clarification…
    - What was the scope of that “medium risk”? (Was it even a risk?)
    - Is that a calibrated estimate?
    - What does “medium” mean?
    - Does it represent best case, worst case, or something else?
  - Socializing the need for higher quality risk measurement standards and practices

Why it matters…



When it comes to risk measurement…

You get what you pay for



Everything should be made as simple as possible, but not any simpler.

Albert Einstein

The FAIR Institute

- Nonprofit dedicated to building a community of experts in more evolved and effective risk management methods
- No cost to join
- Over 1700 members to-date
- Very active blog and numerous white papers
- Soon will offer a free online FAIR tool and pre-defined university curriculum
- Local chapters in large cities (e.g., Chicago, NYC, San Francisco, Washington DC, Toronto)
- Several active workgroups
  - Cyber risk management
  - Data utilization
  - Operational risk
  - University educators

2nd Annual FAIR Conference

- When: Oct 16 & 17
- Where: Dallas, TX
- Same week/location as the RSA Charge conference (RSA is a sponsor of FAIRCon)
- Register thru the fairinstitute.org website

The Open Group

- Professional certification for FAIR practitioners
- Resources for certification prep and for applying FAIR
- Trainer accreditation process
- Continually developing new resources

Resources

- The FAIR Institute
  - http://www.fairinstitute.org
- The Open Group
  - http://www.opengroup.org/standards/security
- Measuring and Managing Information Risk: A FAIR Approach
  - amazon.com
- http://www.RiskLens.com/resources

Questions?