An Introduction to FAIR

Jack Jones
Chairman
FAIR Institute

How much cyber risk does your organization have?

How much less (or more) risk will it have if…?

Typical risk assessment practices don’t enable us to reliably answer these questions.

The risk landscape in a nutshell…

Complex

Dynamic

Limited Resources

…which makes effective prioritization an absolute necessity.

Two fundamental truths about prioritization…

Prioritization is always based on some form of comparison

Comparisons are always based on some form of measurement

The more reliable the measurement, the better your comparisons and priorities will be.

So, how good is the cybersecurity profession at prioritizing?

Between 70% and 90% of “high risk” findings aren’t, in fact, high risk.

No organization I’ve encountered in the past 3 years has correctly identified their top 10 risks.

Prioritizing Effectively

Three criteria for reliably accurate risk measurement…

1. Clarity about what's being measured
2. An accurate risk model
3. Data

Getting clarity

Which of the following are risks?

- Disgruntled insiders
- Reputation
- Untested recovery process
- Network shares containing sensitive consumer information
- Weak passwords
- Cyber criminals

Actually, none of them are risks

- Disgruntled insiders — Threat community
- Reputation — Asset
- Untested recovery process — Deficient control
- Network shares containing sensitive consumer information — Assets
- Weak passwords — Deficient control
- Cyber criminals — Threat community

The classic formula for risk

Risk = Likelihood x Impact

Likelihood and Impact of what?

Loss Event Scenarios

These aren’t loss events

You can only assign likelihood and impact to loss event scenarios.

- Disgruntled insiders
- Reputation
- Untested recovery process
- Network shares containing sensitive consumer information
- Weak passwords
- Cyber criminals

These aren’t loss event scenarios (risks).

A measurement example

How fast are they going?

Qualitatively

Challenges…

- Is your “Fast” the same as mine?
- Which car am I referring to?
  - One in particular? (Slowest? Fastest?)
  - An average for all of them?
- Which part of the track am I referring to?
  - Corners?
  - The straightaway?
  - Average over the entire track?
  - This lap, or an average for the entire race?

Measuring speed

Requires three elements:

1. The scope of what's being measured
   - Which car(s)?
   - Which part of the track?
   - Which lap(s)?

2. An analytic model
   - What data? (time, distance)
   - How to apply the data? (speed = distance/time)

3. Data

Measuring risk

Every risk measurement involves three elements:

1. The scope of what's being measured
   - What asset?
   - What threat?
   - Which vector/method?
   - What type of event (e.g., C, I, A)?
2. An analytic model (e.g., FAIR)
   - What data?
   - How to apply the data?
3. Data

Example of a clearly scoped risk (a loss event scenario)

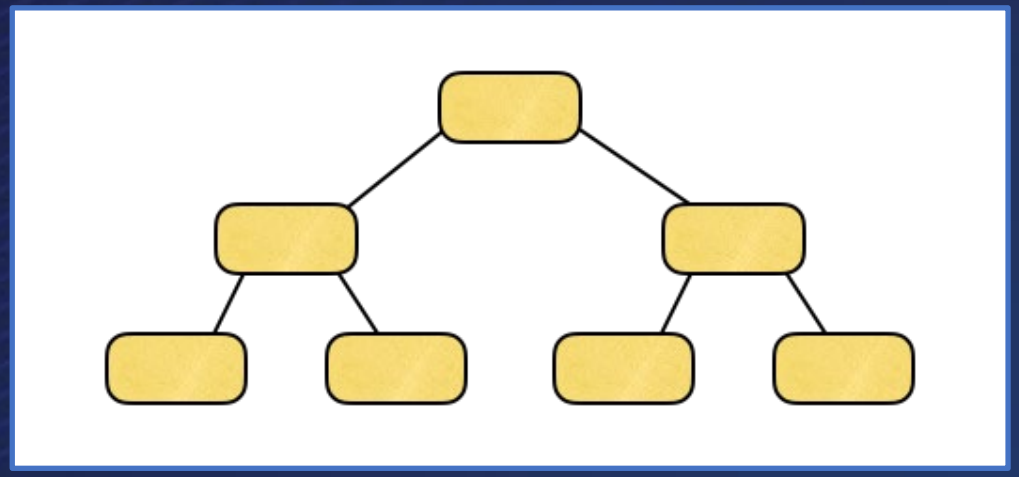
Outage of key business systems due to cybercriminals performing a ransomware attack via a phishing e-mail.

Asset
Threat
Effect
Vector
Method

Without clear scoping, the odds of measuring risk accurately are much lower…

…regardless of whether you're doing qualitative or quantitative measurement

Models

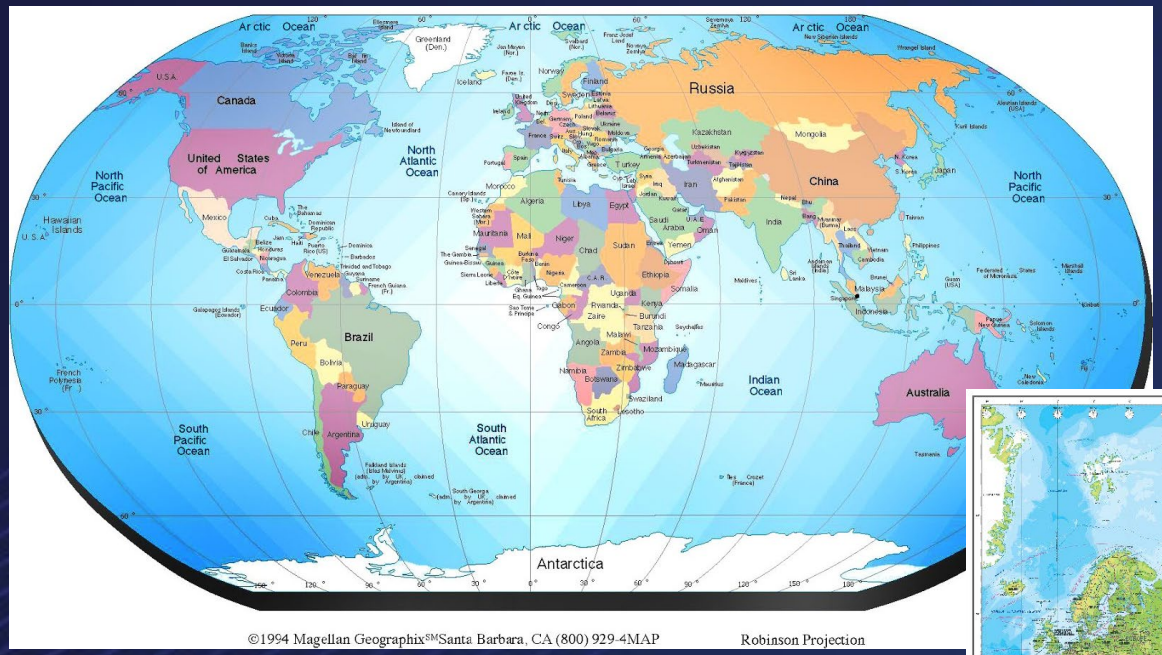


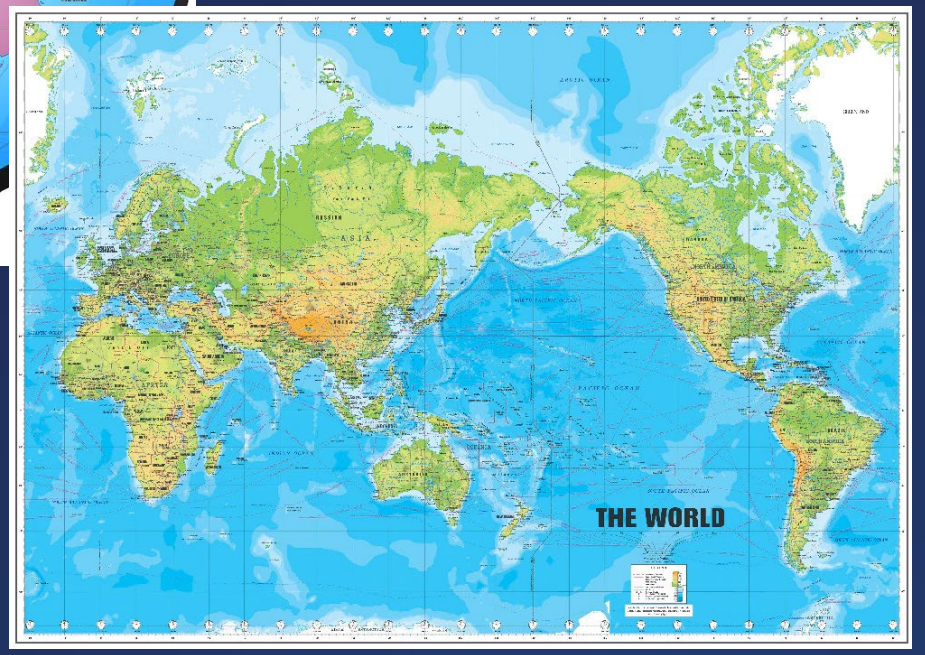
“All models are wrong, but some are useful.”

George Box

But there are different types and degrees of “wrongness”…

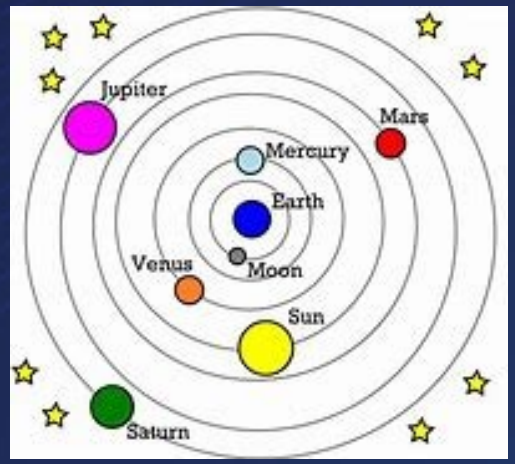
“Wrong” models…





Wrong, in that they aren’t perfect replicas.

A different kind of wrong…



A broken risk measurement model (half of one, anyway)

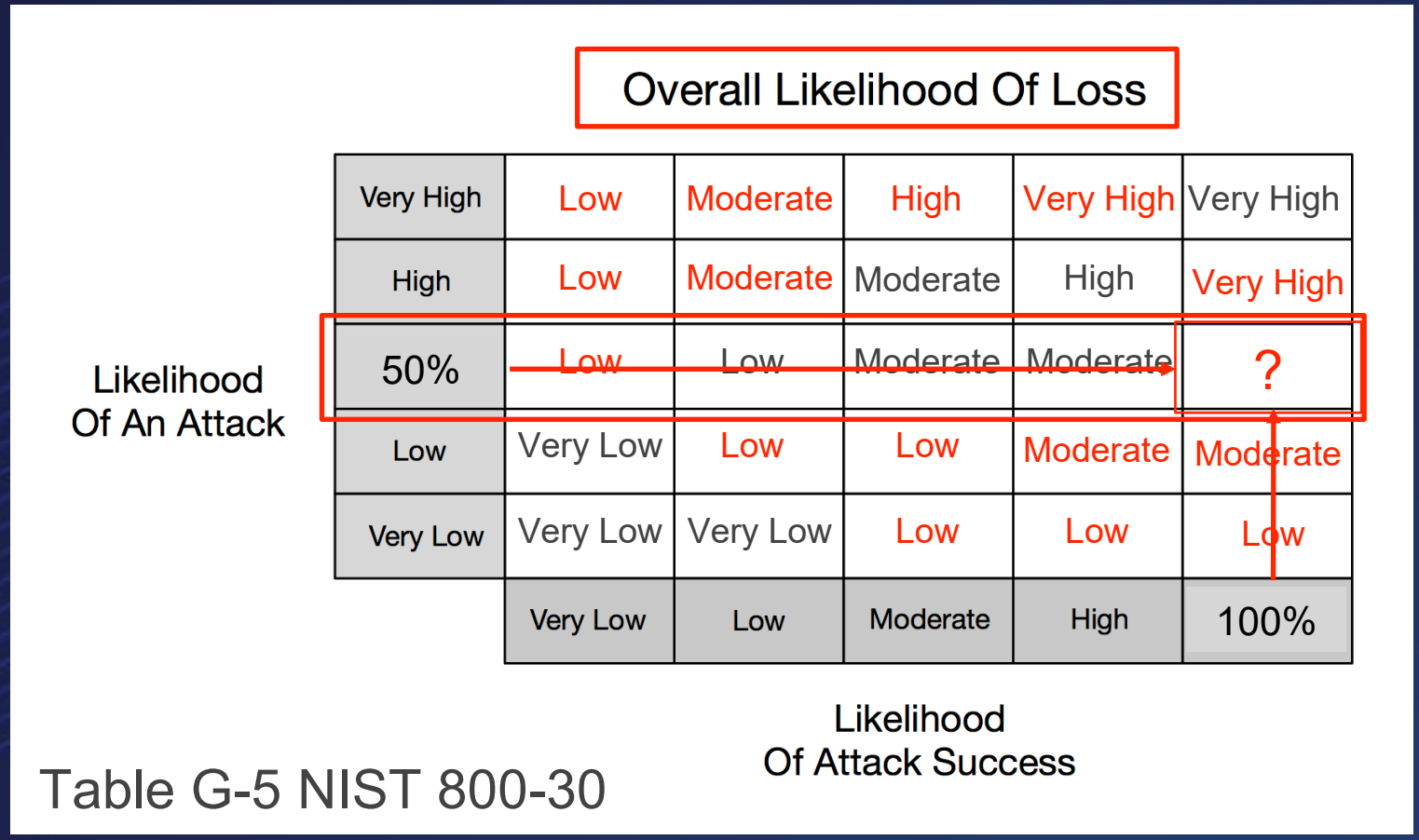
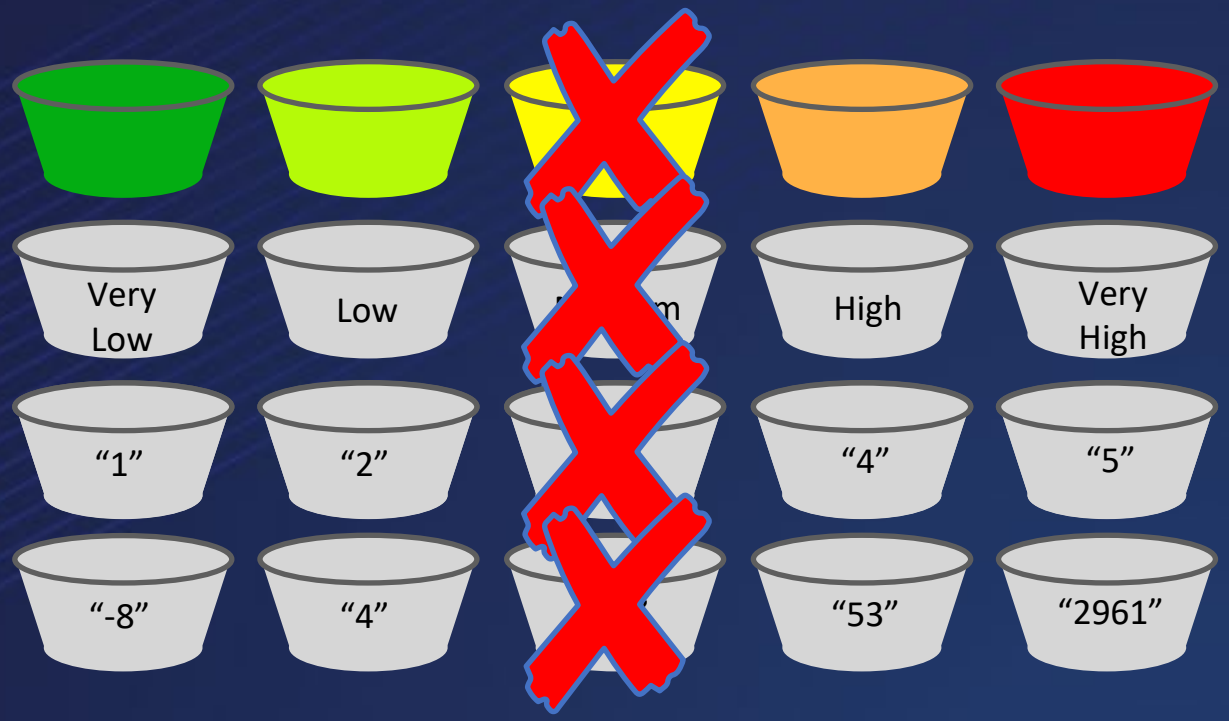


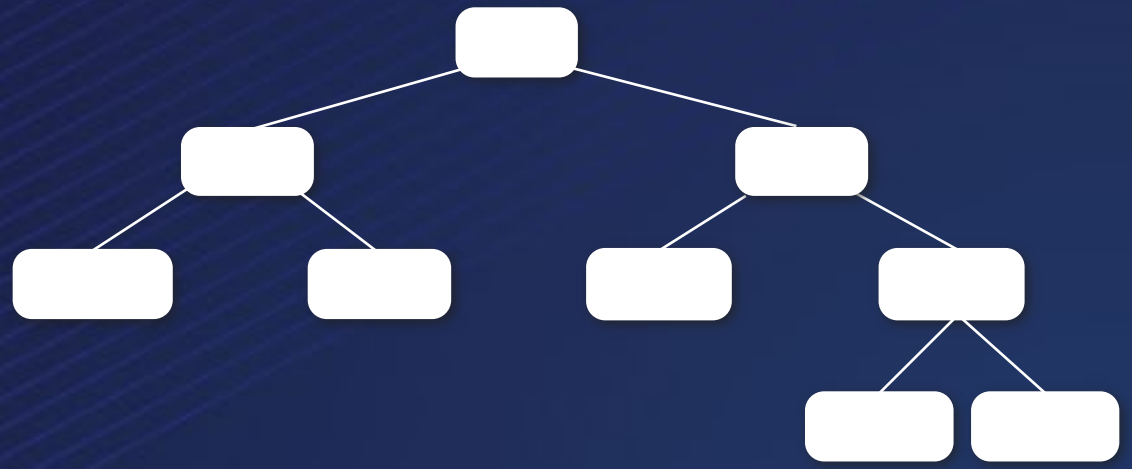
Table G-5 NIST 800-30

Ordinal numbers are not quantitative values

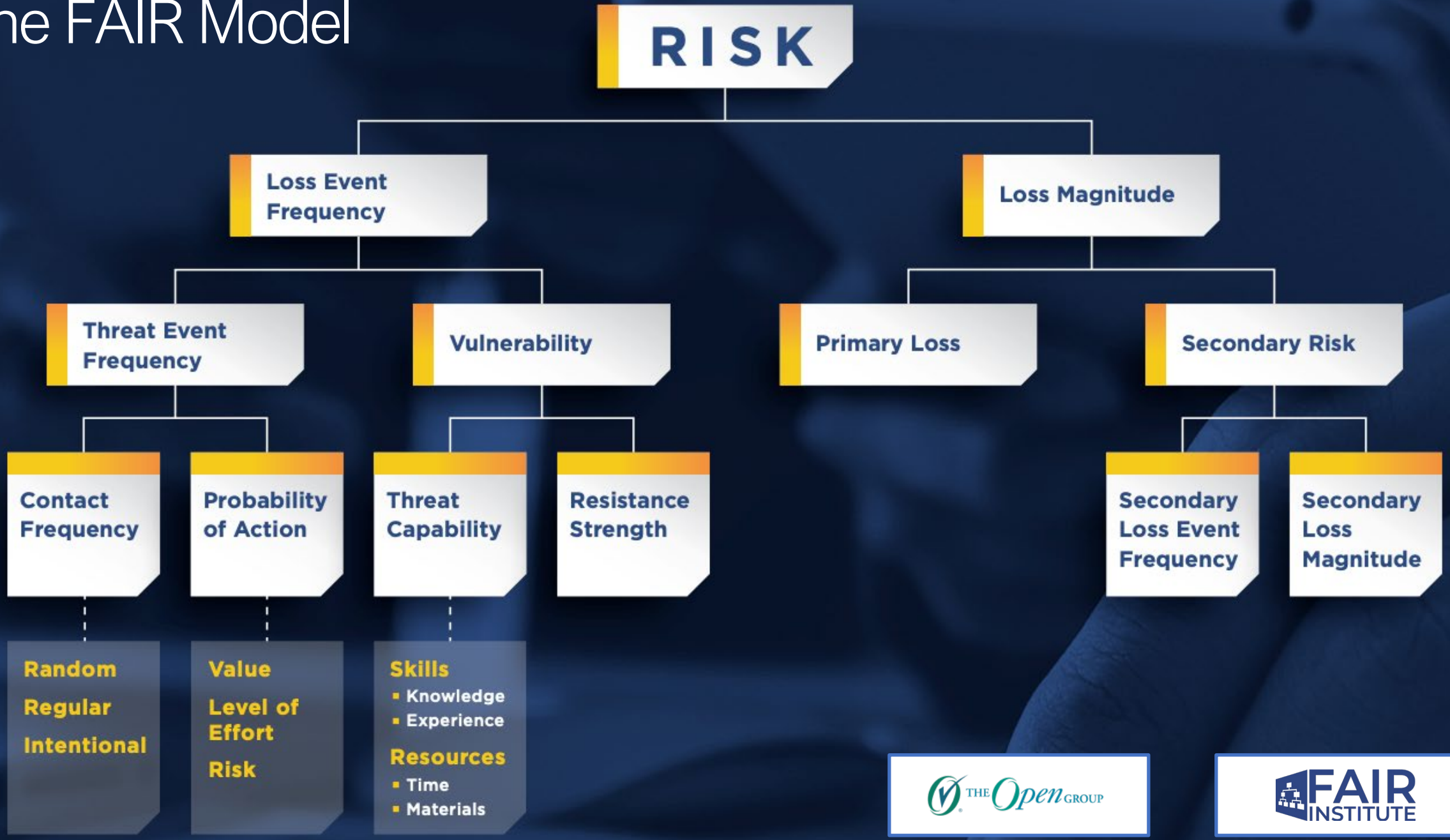
(Green x Yellow) / Red = ?



The FAIR Model



The FAIR Model



THE Open GROUP

FAIR INSTITUTE

DEFINITIONS:

RISK: The probable frequency and probable magnitude of future loss

LOSS EVENT FREQUENCY: The frequency, within a given timeframe, that loss is expected to occur

THREAT EVENT FREQUENCY: The frequency, within a given timeframe, that threat agents are expected to act in a manner that could result in loss

VULNERABILITY: The probability that a threat event will become a loss event

THREAT CAPABILITY: The level of force a threat agent is able to apply

RESISTANCE STRENGTH: A measure of how difficult it is for a threat actor to inflict harm (a.k.a. difficulty)

SECONDARY LOSS EVENT FREQUENCY: The percentage of time that secondary stakeholders are likely to react negatively to an event

FORMS OF LOSS:

PRODUCTIVITY LOSS: Loss that results from an operational inability to deliver products or services

RESPONSE COSTS: Loss associated with the costs of managing an event

REPLACEMENT COSTS: Loss that results from an organization having to replace capital assets

COMPETITIVE ADVANTAGE LOSS: Losses resulting from intellectual property or other key competitive differentiators that are compromised or damaged

FINES AND JUDGMENTS: Fines or judgments levied against the organization through civil, criminal, or contractual actions

REPUTATION DAMAGE: Loss resulting from an external stakeholder perspective that an organization's value has decreased and/or that its liability has increased

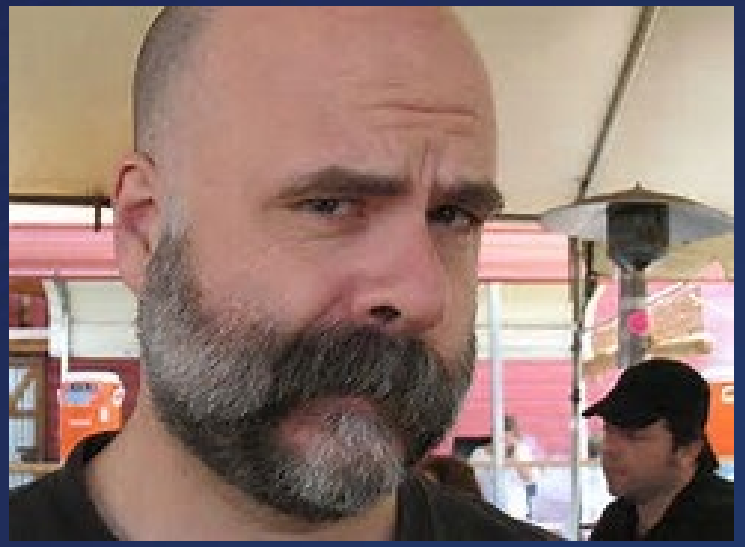
ANALYSIS SCOPING:

1. Clearly understand & describe the loss event
2. Identify the asset(s)
3. Identify relevant threat(s)
4. Define Effect: C-I-A

CALIBRATION:

- Start with the absurd
- Consider what you DO know
- Decompose the problem
- Identify / challenge your assumptions
- Consider where data may exist
- Seek out SMEs
- Focus on accuracy rather than high precision

But what about data?



“We don’t have enough data.”

- “You have more data than you think you do.”
- “You need less data than you think you do.”

Douglas Hubbard

Author of “How to Measure Anything”

The problem of uncertainty…

How tall am I?

Uncertainty is inevitable. It's simply a matter of whether it's accounted for in measurement inputs and outputs.

Using ranges and distributions to faithfully reflect uncertainty is crucial for accurate quantitative risk measurement.

Communicating Effectively

How much do they really understand?

Which of these will most executives understand?

- A marketing campaign that is expected to generate $1M to $2.5M in additional revenue over the next 12 months.
- A cost-cutting initiative that will trim approximately $1.3M in expenses this year.
- A cybersecurity initiative that will enable early detection of breaches, improving this from “High risk” to “Medium risk”.

Enabling informed comparisons

- A marketing campaign that is expected to generate $1M to $2.5M in additional revenue over the next 12 months.
- A cost-cutting initiative that will trim approximately $1.3M in expenses this year.
- A cybersecurity initiative that will enable early detection of breaches, reducing loss exposure by between $7M and $10M.

Example Use-Case

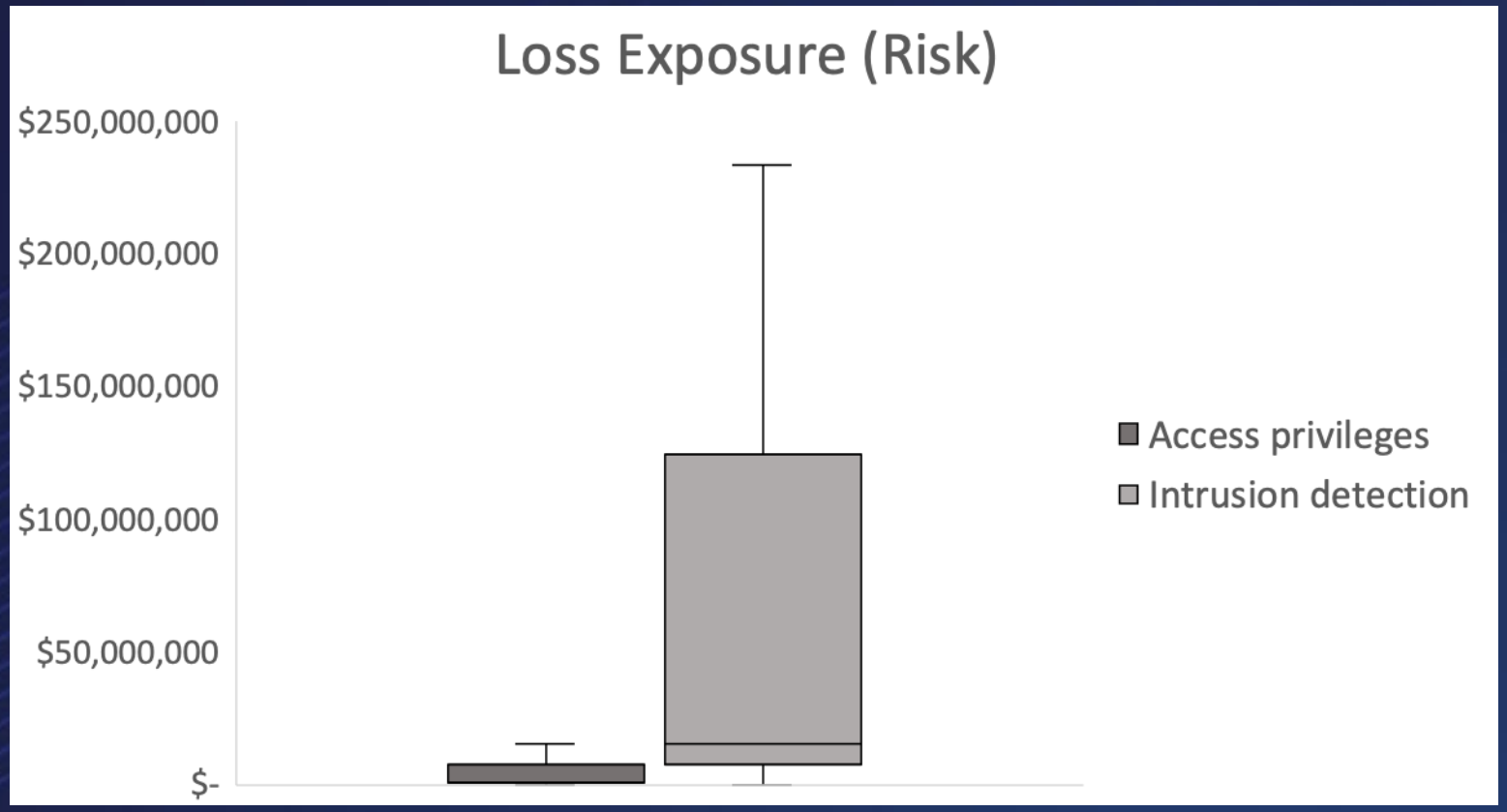
For example — which should we fix first?

An audit discovered that privileges are not consistently being updated for user accounts with access to a customer service application containing credit card numbers.

A security assessment determined that the organization was unlikely to be able to identify when a cyber criminal breaches its network perimeter.

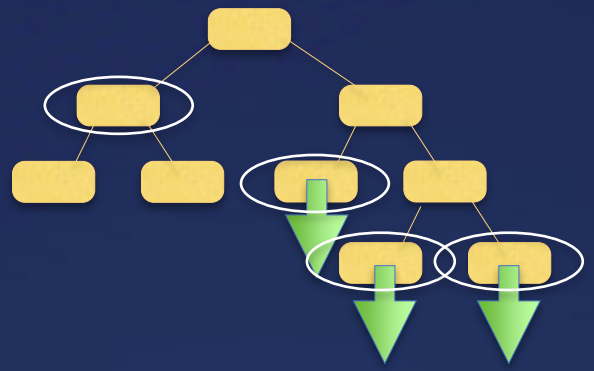
Both were identified as “high risk” using typical assessment methods.

Analytic results using FAIR



What changes when we apply strong detection?

- Loss Event Frequency doesn't change
- Loss Magnitude changes:
  - Primary loss goes down because of earlier detection and simpler forensics.
  - Secondary loss event frequency goes down because there are better odds of intervening before customer data is compromised.
  - Secondary loss magnitude goes down because the threat actor is less likely to have time to find the mother load.
- Only the Most Likely value changes (not Min or Max)!



Wrapping up

Managing cyber risk effectively…

- Accurate prioritization is crucial to effective cyber risk management.
- Prioritization is always based on measurements. The better your measurement, the better your ability to prioritize.
- Three fundamental criteria for reliable risk measurements:
  - Clarity: You can't reliably measure what you haven't clearly defined
  - An accurate model: All models are imperfect — but some are fundamentally broken
  - Data: Data will always have uncertainty. The key is to faithfully account for and communicate uncertainty.
- Those criteria are true for qualitative or quantitative risk measurements…
- Until we're able to prioritize reliably, we won't have good odds against the threats we face.

FAIR Resources

- The FAIR Institute (www.fairinstitute.org)
- The Open Group (www.opengroup.org/certifications/openfair)
- RiskLens (www.risklens.com/resources)
- Measuring and Managing Information Risk: A FAIR Approach (www.amazon.com)