Changing Executive Priorities and Investments in Cybersecurity

Jack Jones
Chairman, FAIR Institute

What cybersecurity professionals want…

For cybersecurity to be on an even playing field with other business priorities

What executives want…

To understand the value of their investments in security

Prioritizing

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 normalized the measurement, the better comparisons and priorities will be.

Keep in mind…

People generally prioritize their efforts based on how they're incentivized.

What are the two most common things executives are incentivized on?

Revenue

$

Expenses

$

Which of these is the highest priority?

- 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”.

Measuring Risk Quantitatively

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

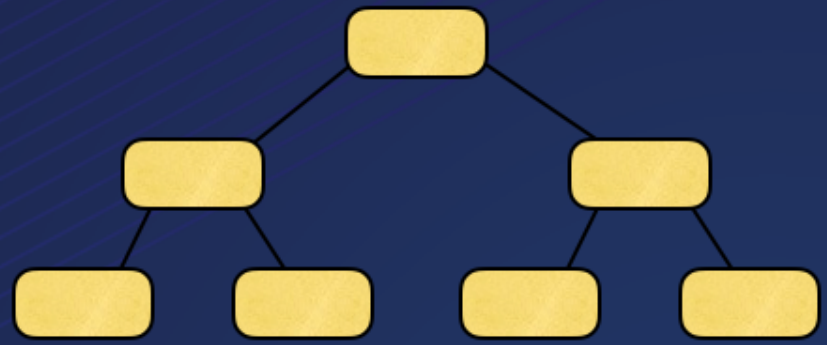
Every risk measurement involves three elements:

1. The scope of what's being measured
   - What asset?
   - What threat?
   - Which vector?
   - Which controls are relevant?
   - 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

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

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

The Model Element



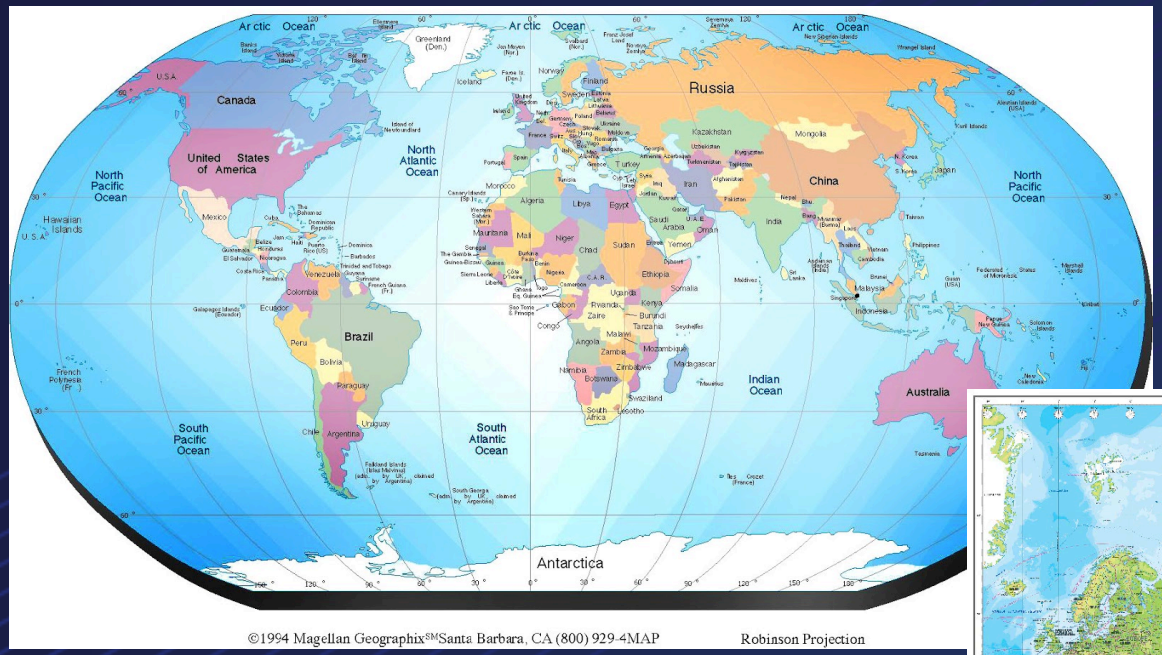
A model is a simplified representation of reality
used to simulate, explain, and make predictions.

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

George Box

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

Example “wrong” models…



A broken risk model (half of one, anyway)

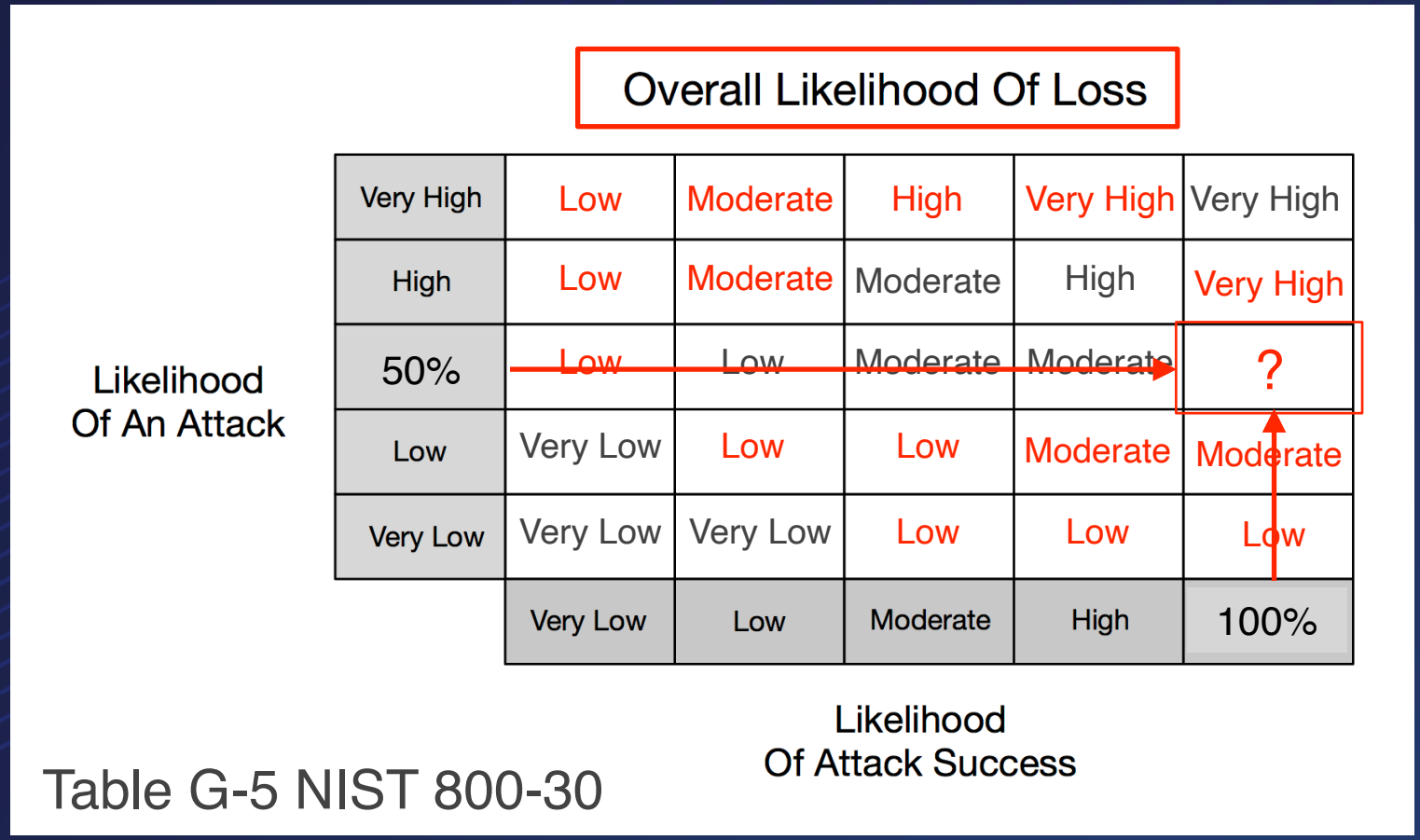
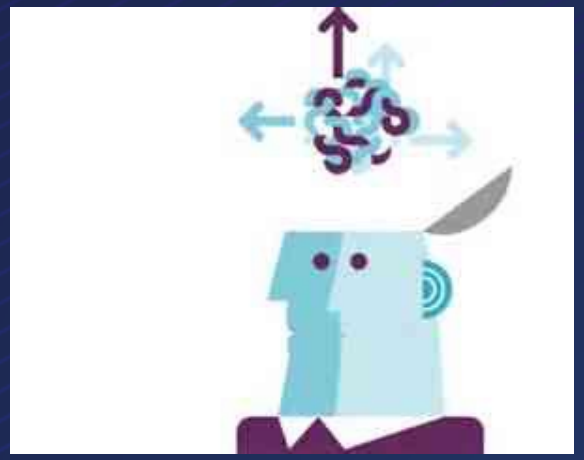


Table G-5 NIST 800-30

What is the most commonly used cyber risk measurement model?



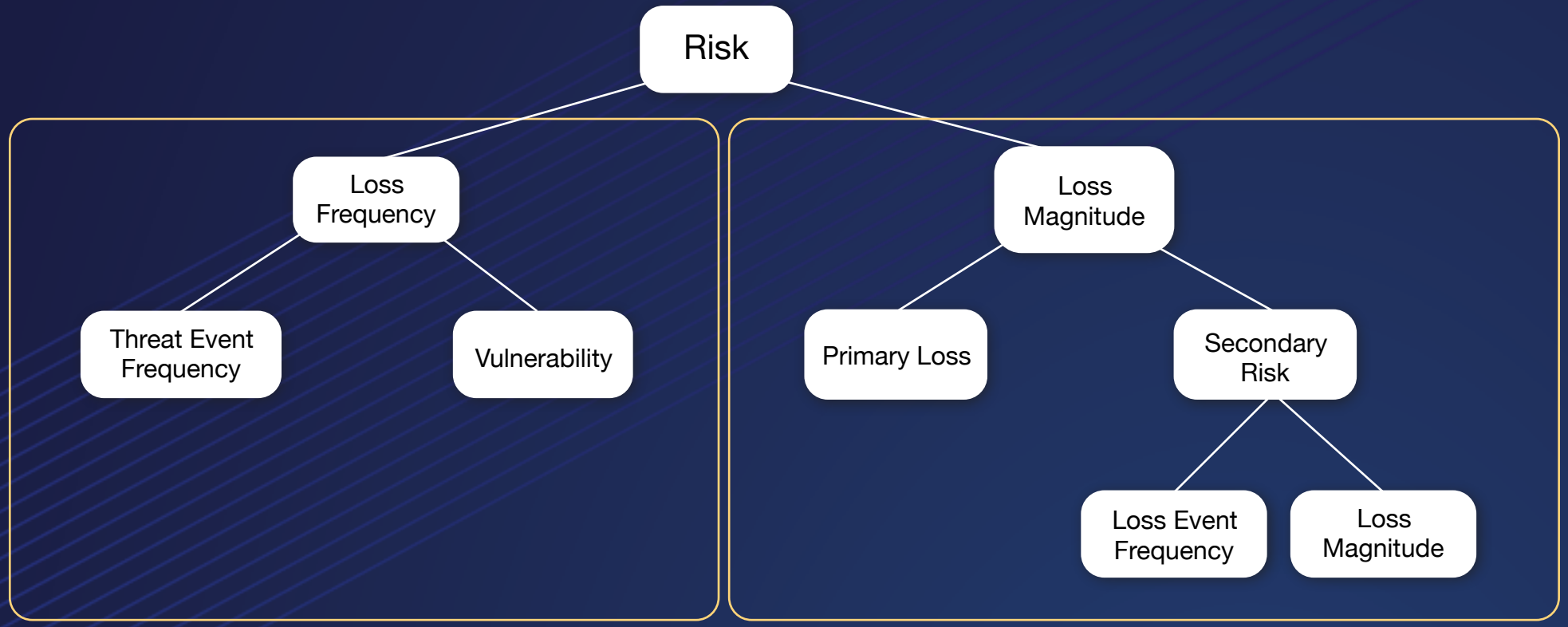
Mental models

What assumptions?

What data?

What formula?

The FAIR Model



Loss Event Frequency

Loss Magnitude

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”

For any risk analysis…

- What data do we need? The risk model tells us this
- Where do we get them? The scope tells us this
- How do we apply them? The model tells us this

If the analysis is scoped clearly and you're using a well-defined model, then data will be far less challenging to gather and use.

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.

Back to where we started

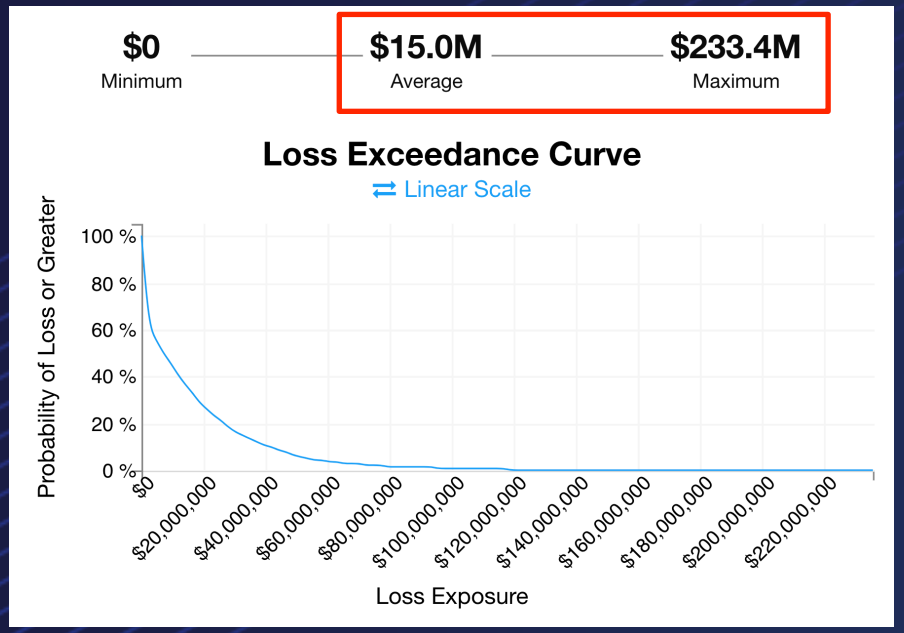
Which of these is the highest priority?

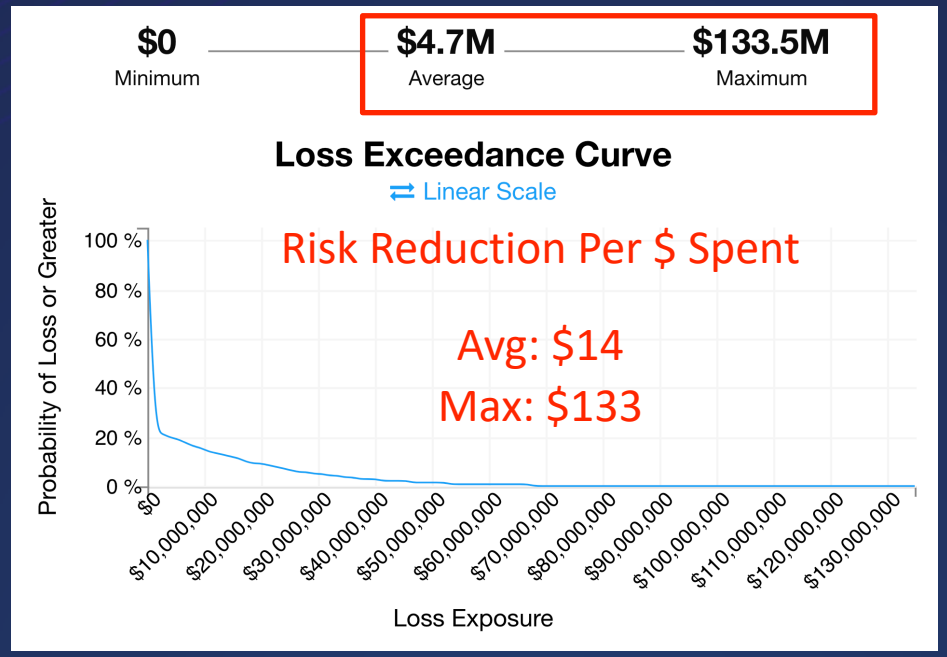
- A marketing campaign that is expected to generate $1M to $2.5M in additional revenue over the next 12 months.
- A cost-cutting initiative that will trim approximately $1.3M in expenses this year.
- A cybersecurity initiative that will enable early detection of breaches, reducing average annualized loss exposure by approximately $10M at a 1st year cost of approximately $750k.

Example analysis result (breach detection)

A risk reduction solution was identified that was going to cost $750k in year 1, and approx. $300k yearly thereafter.

Current State





Informing ~~Changing~~ Executive Priorities and Investments in Cybersecurity

Benefits

- Enables economic expression of risk and risk reduction, which enables more effective prioritization. Executives get their wish.
- Increases cybersecurity's perceived value and executive support when warranted — i.e., the playing field is leveled. Cybersecurity professionals get their wish.